



FY 2022 Homeland Security Grant Program

Michigan Supplemental Guidance

This page intentionally left blank

Table of Contents

Preface	1
Program Purpose	2
Description of Programs	2
Alignment of HSGP to the National Preparedness System	3
Homeland Security Grant Program Funding Requirements.....	4
Homeland Security Grant Program Restrictions	9
FY 2022 HSGP Funding Guidelines.....	15
FY 2022 HSGP-SHSP Investments	25
Appendix A: Summary of the National Preparedness Goal	35
Appendix B: Summary of the Core Capabilities	37
Appendix C: Stakeholder Preparedness Review Functional Gaps.....	40
Appendix D: FY 2022 Programs - Allowable Program Activities	47
Appendix E: Subrecipient Administrative Process	50
Appendix F: FY 2022 HSGP Project Workbook Checklist	51
Appendix G: FY 2022 Homeland Security Grant Program Document Submission Checklist	54
Appendix H: Discussion on 2 CFR Part 200 Compliance Issues	56
Appendix I: Advance Request Procedures	61
Appendix J: Acronym List.....	63
Appendix K: MSP/EMHSD Points-of-Contact.....	64

Preface

The Fiscal Year (FY) 2022 Homeland Security Grant Program (HSGP) funding priorities are supported in this guidance, as is Michigan's commitment to correct identified capability shortfalls. The Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD) is dedicated to assisting regional partner's implementation of the National Preparedness System (NPS) through the development and sustainment of core capabilities identified in the National Preparedness Goal (NPG). Allowable costs support efforts to build and sustain core capabilities across the prevention, protection, mitigation, response, and recovery mission areas. HSGP-funded activities must support the NPG (see Appendix A, Summary of National Preparedness Goal) and align to the Federal FY 2022 HSGP Notice of Funding Opportunity, the FY 2022 Preparedness Grants Manual, and Michigan's FY 2022 HSGP Investment Justifications.

The investment descriptions included in this guidance document are the FY 2022 State Homeland Security Program (SHSP) investments submitted to the Department of Homeland Security (DHS) / Federal Emergency Management Agency (FEMA), Grants Program Directorate (GPD). The FY 2022 Urban Areas Security Initiative (UASI) Investment Justification is available to the UASI Region in a separate document. However, the HSGP guidance contained herein is applicable to the SHSP and UASI programs.

Michigan's FY 2022 SHSP and UASI investments are based on data derived from capability assessments resulting from the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) process. Capability-based investment planning allows regional homeland security partners to target funding to priority areas of the greatest concern for each region.

MSP/EMHSD will provide continued support to regional partners with implementation of statewide homeland security initiatives and the NPS throughout the FY 2022 period of performance.

Please note: This guidance is intended to provide supplemental information regarding administration of the HSGP and is not a complete resource for all potential HSGP funding scenarios or reporting requirements.

Program Purpose

The FY 2022 HSGP is comprised of three grant programs that constitute the DHS/FEMA focus on enhancing the ability of state, local, tribal, and territorial governments, as well as nonprofits, to prevent, protect against, respond to, and recovery from terrorist attacks. These grant programs are part of a comprehensive set of measures authorized by Congress and implemented by DHS to help strengthen the nation's communities against potential terrorist attacks.

The FY 2022 HSGP programs include:

- 1.State Homeland Security Program (SHSP)
- 2.Urban Areas Security Initiative (UASI); and
- 3.Operation Stonegarden (OPSG)

Together, these grant programs fund a range of activities including planning, organization, equipment purchases, training, and exercises across all core capabilities and mission areas.

Please note: This guidance document does not address OPSG. Refer to the Federal FY 2022 HSGP Notice of Funding Opportunity for information relating to OPSG.

Description of Programs

The HSGP includes a suite of risk-based grants to assist State, Local, Tribal, and Territorial efforts in preventing, preparing for, protecting against, responding to, and recovering from acts of terrorism. FEMA's comprehensive suite of grant programs are an important part of the Administration's larger, coordinated effort to strengthen homeland security preparedness. HSGP is one tool among a set of initiatives to help prepare the nation for threats and hazards that pose the greatest risk to the security of the United States.

State Homeland Security Program (SHSP)

The SHSP assists state, local, tribal, and territorial efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.

Use of SHSP funds must be consistent with and directly support capability sustainment or implementation of initiatives designed to address capability shortfalls identified through the Threat and Hazard Identification and Risk Assessment (THIRA) and the Stakeholder Preparedness Review (SPR) process and align to one of the State's approved FY 2022 SHSP Investments (see FY 2022 HSGP - SHSP Investments section of this document for additional information). Linkages between specific projects undertaken with SHSP funds and specified documents will be highlighted and monitored through required reporting mechanisms.

Urban Area Security Initiative (UASI)

The UASI assists high-threat, high-density Urban Areas efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.

Use and allocation of all grant funds available through the UASI must focus on the investments identified in the Urban Area's FY 2022 Investment Justification and support capability sustainment or address shortfalls identified through the Urban Areas THIRA and SPR process.

Operation Stonegarden (OPSG)

OPSG supports enhanced cooperation and coordination among Customs and Border Protection (CBP), United States Border Patrol (USBP) and federal, state, local, tribal, and territorial law enforcement agencies to improve overall border security. OPSG provides funds to support joint efforts to secure the United States borders along routes of ingress/egress to and from international borders, including travel corridors in states bordering Mexico and Canada as well as states and territories with international water borders. Refer to the Department of Homeland Security's FY 2022 Homeland Security Grant Program Notice of Funding Opportunity for additional information on OPSG.

Alignment of HSGP to the National Preparedness System

The Nation uses the NPS to build, sustain, and deliver core capabilities to achieve the NPG. Subrecipients will use the National Preparedness System to support their efforts to build, sustain, and deliver these core capabilities. The components of the National Preparedness System are Identifying and Assessing Risk; Estimating Capability Requirements; Building and Sustaining Capabilities; Planning to Deliver Capabilities; Validating Capabilities; and Reviewing and Updating.

As the National Preparedness System matures, FEMA is getting better data on our capabilities as a nation that can be used to drive our focus and our resources at all levels. States, territories, and urban areas provide annual data on their proficiency across 32 core capabilities through the Threat and Hazard Identification and Risk Assessment, Stakeholder Preparedness Review, after-action reports, and other preparedness data. This data feeds into the National Preparedness Report and forms a shared national picture of needs relative to capability gaps, including what threats and hazards are posing the greatest risks and what core capabilities are most in need of improvement or sustainment. Analytic results help shape prioritization decisions at FEMA and across the nation to make sure time and resources are focused in the right areas.

The HSGP provides financial support to help build, sustain, and deliver core capabilities identified in the NPG. A key focus and requirement of the HSGP is to prevent terrorism and other catastrophic events and to prepare the Nation for the threats and hazards that pose the greatest risk to the security of the United States, including risks along the Nation's borders. When applicable, funding should support deployable assets that can be used anywhere in the Nation through automatic assistance and mutual aid agreements, including, but not limited to, the Emergency Management Assistance Compact (EMAC).

The HSGP supports investments that improve the ability of jurisdictions nationwide to:

- Prevent a threatened or an actual act of terrorism;
- Protect citizens, residents, visitors, and assets against the greatest threats that pose the greatest risk to the security of the United States;
- Mitigate the loss of life and property by lessening the impact of future catastrophic events;

- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident; and
- Recover through a focus on the timely restoration, strengthening, accessibility and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident, and do so in a manner that engages the whole community while ensuring the protection of civil rights.

Homeland Security Grant Program Funding Requirements

In 2022, DHS is focused on the criticality of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other threats to our national security. The threats to our nation have evolved during the past two decades. We now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, and threats from domestic violent extremists who currently pose the greatest terrorism threat to the nation¹. Therefore, for FY 2022, DHS identified six priority areas related to the most serious threats to the nation. Subrecipients must use HSGP funds to address these threats.

Given the evolving national security threat landscape, DHS/FEMA has evaluated the national risk profile and set priorities that help inform appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2022, six priority areas attract the most concern. Due to the unique threats the nation faces in 2022, DHS/FEMA determined that a total of 30 percent of SHSP and UASI award funds must be allocated across these six priority areas. As indicated below, four of the priorities have minimum spend requirements totaling 12 percent of SHSP and UASI awards. Subrecipients have the flexibility to allocate the remaining 18 percent across the priorities. The following are the six priority areas for FY 2022, along with the minimum corresponding percentage of SHSP and UASI funds that are required:

1. Enhancing the protection of soft targets/crowded places – 3 percent;
2. Enhancing information and intelligence sharing and cooperation with federal agencies, including the Department of Homeland Security (DHS) – 3 percent;
3. Combating domestic violent extremism (new) – 3 percent;
4. Enhancing cybersecurity – no minimum percent;
5. Enhancing community preparedness and resilience – 3 percent; and
6. Enhancing election security – no minimum percent.

All subrecipients are required to allocate funding to these priority areas and each project must be reviewed and approved by FEMA prior to any expenditures. This requirement applies to SHSP and UASI funds.

Exact dollar amounts per priority area that required for each subrecipient are included in the subrecipient grant agreement.

¹ Strategic Intelligence Assessment and Data on Domestic Terrorism. Federal Bureau of Investigation and Department of Homeland Security. May 2021.

Cybersecurity

Cybersecurity projects must support the security and functioning of critical infrastructure and core capabilities as they relate to preventing, preparing for, protecting against, or responding to acts of terrorism.

Additional resources and information regarding cybersecurity are available through the [CYBERSECURITY | CISA](#) and [Cybersecurity Framework | NIST](#).

Soft Targets and Crowded Places

Soft targets and crowded places are increasingly appealing to terrorists and other extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities.

Additional resources and information regarding securing soft targets and crowded places are available through the [Securing Public Gatherings | CISA](#).

Intelligence and Information Sharing

Effective homeland security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments, and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Additional resources and information regarding collaboration and information sharing are available through the Department's [Office of Intelligence and Analysis](#).

Combatting Domestic Violent Extremism

As stated in the October 2020 DHS Homeland Threat Assessment, domestic violent extremists, including ideologically motivated lone offenders and small groups, present the most persistent and lethal terrorist threat to the Homeland. These violent extremists capitalize on social and political tensions, which have resulted in an elevated threat environment. They utilize social media platforms and other technologies to spread violent extremist ideologies that encourage violence and influence action within the United States. The COVID-19 pandemic has further created an environment that may lead to accelerated mobilization to targeted violence and/or radicalization to domestic terrorism, including driving lawful protests to incite violence, intimidate targets, and promote their violent extremist ideologies.

Additional information is available through the [Center for Prevention Programs and Partnerships | Homeland Security \(dhs.gov\)](#).

Community Preparedness and Resilience

Community organizations are the backbones of American civic life, both during “blue skies” and in the aftermath of terrorist attacks. Community organizations, such as homeless shelters, food banks, public libraries, faith-based institutions, and nonprofit medical providers must have the capabilities to withstand acts of terrorism and provide essential services, especially to members of underserved communities, in the aftermath of an attack. In addition, individual citizens, and volunteer responders, such as Community Emergency Response Teams, may also be on the scene after a terrorist attack. The ability of these volunteers to provide assistance to their fellow citizens is paramount to a community’s resilience. This National Priority Area will bolster community preparedness and resilience by investing in local, community-driven capabilities.

Additionally, equity in emergency management requires proactively prioritizing actions that reinforce cultural competency, accessibility, and inclusion, as well as reflect the historical context of specific groups of people. To that end, subrecipients are strongly encouraged to explore how SHSP- and UASI-funded activities can address the needs of underserved, at-risk communities to help ensure consistent and systematic, fair, just, and impartial treatment of all individuals before, during, and after a disaster.

Additional resources and information regarding community preparedness and resilience are available through [Individuals and Communities | FEMA.gov](#).

Election Security

In January 2017, DHS designated the infrastructure used to administer the Nation’s elections as critical infrastructure. This designation recognizes that the United States’ election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Securing election infrastructure and ensuring an election free from foreign interference are national security priorities. Threats to election systems are constantly evolving, so defending these systems requires constant vigilance, innovation, and adaptation.

Additional resources and information regarding election security are available through the [Election Security Library | CISA](#).

FY 2022 SHSP and UASI Funding Priorities

National Priority Alignment to Core Capabilities

The table below provides a breakdown of the FY 2022 SHSP and UASI priorities showing the core capabilities enhanced as well as examples of eligible project types for each area. The DHS/FEMA anticipate that in future years, national priorities will continue to be included and will be updated as the threats evolve and as capability gaps are closed.

Priority Area	Core Capabilities	Lifelines	Example Projects
Enhancing Cybersecurity	<ul style="list-style-type: none">▪ Cybersecurity.▪ Intelligence and information sharing.▪ Planning.	Safety and Security	<ul style="list-style-type: none">▪ Cybersecurity risk assessments.▪ Migrating online services to the “.gov” internet domain.

	<ul style="list-style-type: none"> Public information and warning. Operational coordination. Screening, search, and detection. Access control and identity verification. Supply chain integrity and security. Risk management for protection programs and activities. Long-term vulnerability reduction. Situational assessment. Infrastructure systems. Operational communications. 		<ul style="list-style-type: none"> Projects that address vulnerabilities identified in cybersecurity risk assessments. <ul style="list-style-type: none"> Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity training and planning.
Priority Area	Core Capabilities	Lifelines	Example Projects
Enhancing the Protection of Soft Targets/Crowded Places	<ul style="list-style-type: none"> Operational coordination. Public information and warning. Intelligence and information sharing. Interdiction and disruption. Screening, search, and detection. Access control and identity verification. Physical protective measures. Risk management for protection programs and activities. 	Safety and Security	<ul style="list-style-type: none"> Operational overtime. Physical security enhancements. <ul style="list-style-type: none"> Closed-circuit television (CCTV) security cameras. Security screening equipment for people and baggage. Lighting. Access controls. Fencing, gates, barriers, etc. Unmanned aircraft system detection technologies.
Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies, including DHS	<ul style="list-style-type: none"> Intelligence and information sharing. Interdiction and disruption. Planning. Public information and warning. Operational coordination. Risk management for protection programs and activities. 	Safety and Security	<ul style="list-style-type: none"> Fusion center operations (Fusion Center project will be required under this investment, no longer as a stand-alone investment). Information sharing with all DHS components; fusion centers; other operational, investigative, and analytic entities; and other federal law enforcement and intelligence entities. Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition, assessment, analysis, and mitigation. Identification, assessment, and reporting of threats of violence. Joint intelligence analysis training and planning with DHS officials and other entities designated by DHS.
Combating Domestic Violent Extremism	<ul style="list-style-type: none"> Interdiction and disruption. Intelligence and information sharing. 	Safety and Security	<ul style="list-style-type: none"> Open-source analysis of disinformation and misinformation, targeted violence, and

	<ul style="list-style-type: none"> ▪ Planning. ▪ Public information and warning. ▪ Operational coordination. ▪ Risk management for protection programs and activities. 		<p>threats to life, including tips/leads, and online/social media-based threats.</p> <ul style="list-style-type: none"> ▪ Sharing and leveraging intelligence and information, including open-source analysis. ▪ Execution and management of threat assessment programs to identify, evaluate, and analyze indicators and behaviors indicative of domestic violent extremists. ▪ Training and awareness programs (e.g., through social media, suspicious activity reporting [SAR] indicators and behaviors) to help prevent radicalization. ▪ Training and awareness programs (e.g., through social media, SAR indicators and behaviors) to educate the public on misinformation campaigns and resources to help them identify and report potential instances of domestic violent extremism.
Priority Area	Core Capabilities	Lifelines	Example Projects
Enhancing Community Preparedness and Resilience	<ul style="list-style-type: none"> ▪ Planning. ▪ Public Information and Warning. ▪ Community Resilience. ▪ Risk Management for Protection Programs and Activities. ▪ Mass Care Services. ▪ Intelligence and Information Sharing. ▪ Risk and Disaster Resilience Assessment. ▪ Long-term Vulnerability Reduction. 	Safety and Security	<ul style="list-style-type: none"> ▪ Establish, train, and maintain CERT and Teen CERT, with a focus on historically underserved communities. ▪ Local delivery of CERT Train-the-Trainer and CERT Program Manager training. ▪ Provide continuity training to faith-based organizations, local businesses, and community-based organizations. ▪ Partner with local school districts to deliver the Student Tools for Emergency Planning curriculum or other educational programming. ▪ Execute <i>You are the Help Until the Help Arrives</i> workshops. ▪ Target youth preparedness. ▪ Promote community planning, coordination, and integration of children's needs during emergencies. ▪ Community Mapping: identify community resources and characteristics in order to identify gaps in resources, identify hazards and vulnerabilities, and inform action to promote resilience. ▪ Provide training and awareness programs with key stakeholders to educate the public on misinformation and disinformation campaigns.
Enhancing Election Security	<ul style="list-style-type: none"> ▪ Cybersecurity. ▪ Intelligence and Information Sharing. ▪ Planning. ▪ Long-term Vulnerability Reduction. ▪ Situational Assessment. ▪ Infrastructure Systems. 	Safety and Security	<ul style="list-style-type: none"> ▪ Physical security planning support. ▪ Physical/site security measures – e.g., locks, shatter proof glass, alarms, etc. ▪ General election security navigator support. ▪ Cyber navigator support. ▪ Cybersecurity risk assessments, training, and planning.

			<ul style="list-style-type: none"> ▪ Projects that address vulnerabilities identified in cybersecurity risk assessments. ▪ Iterative backups, encrypted backups, network segmentation, software to monitor/scan, and endpoint protection. ▪ Distributed Denial of Service protection. ▪ Migrating online services to the “.gov” internet domain.
--	--	--	--

Homeland Security Grant Program Restrictions

Award Period of Performance

The subrecipient period of performance for this grant is included in the subrecipient grant agreement. Refer to individual grant agreements for exact effective dates.

National Incident Management System (NIMS) Implementation

Subrecipients must ensure and maintain adoption and implementation of NIMS. NIMS guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System. HSGP subrecipients must use standardized resource management concepts for resource typing, credentialing, and an inventory to facilitate the effective identification, dispatch, deployment, tracking, and recovery of resources.

The *NIMS Implementation Objectives for Local, State, Tribal, and Territorial Jurisdictions* clarify the NIMS implementation requirements in FEMA preparedness grant NOFOs. As subrecipients of federal preparedness (non-disaster) grant awards, jurisdictions and organizations must achieve, or be actively working to achieve, all the NIMS Implementation Objectives. The objectives can be found on the NIMS webpage at <https://www.fema.gov/emergency-managers/nims/implementation-training>.

For questions on NIMS implementation, please contact Mr. Henrik Hollaender at 517-898-4225 or HollaenderH@michigan.gov.

Emergency Management Assistance Compact (EMAC) Membership

All assets supported in part or entirely with FY 2022 HSGP funding must be readily deployable and NIMS-typed, when possible, to support emergency or disaster operations per existing EMAC agreements. In addition, funding may be used for the sustainment of core capabilities that, while they may not be physically deployable, support national response capabilities such as Geographic/Geospatial Information Systems, interoperable communications systems, capabilities as defined under the mitigation mission area of the NPG, and fusion centers.

Law Enforcement Terrorism Prevention Activities (LETPA)

Per section 2006 of the Homeland Security Act of 2002, as amended (6 U.S.C. § 607), DHS/FEMA is required to ensure at least 25 percent (25%) of HSGP funds are used for LETPA. **For FY 2022, DHS/FEMA is requiring that at least 30 percent (30%) of grant funding appropriated under the HSGP is used for LETPA.** To meet this requirement, all subrecipients must allocate at least **30 percent** of HSGP funds awarded under SHSP and UASI towards

LETPA. The 30 percent LETPA requirement may be met by funding projects in any combination of the six National Priority Areas and any other investments.

Activities outlined in the National Prevention Framework are eligible for use as LETPA-focused funds. Also, where capabilities are shared with the protection mission area, the National Protection Framework activities are also eligible. Other terrorism prevention activities proposed for funding under LETPA must be approved by the FEMA Administrator.

Personnel Costs

Personnel hiring, overtime, and backfill expenses are permitted under the FY 2022 HSGP for allowable planning, training, exercise, and equipment activities. Subrecipients may not use more than 50% of their total program funds for personnel and personnel-related activities.

In general, the use of HSGP funding to pay for staff and/or contractor regular time or overtime/backfill is considered a personnel cost. See the FY 2022 HSGP Funding Guidelines section of this document for additional information.

Management and Administration

A maximum of 5% of subrecipient HSGP funds awarded may be used to support Management and Administration (M&A) costs associated with implementation of the grant award. Any funds retained are to be used solely for management and administrative purposes associated with the HSGP award. M&A activities are those directly relating to the management and administration of HSGP funds, such as financial management and monitoring.

Multiple Purpose or Dual-Use of Funds

For both SHSP and UASI, many activities which support the achievement of core capabilities related to the national priorities and terrorism preparedness may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. However, all SHSP and UASI funded projects must assist subrecipients in achieving core capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, per section 2008(c) of the Homeland Security Act of 2002 (6 U.S.C. §609(c)).

Role of the THIRA/SPR in the Homeland Security Grant Program

The THIRA includes standardized language to describe threat and hazard impacts that are used to establish capability targets. This allows communities to collect more specific, quantitative information while also providing important context. Through the SPR process, communities collect more detailed and actionable data on their current capabilities and identify capability gaps. Communities then indicate their intended approaches for addressing those gaps and assess the impact of relevant funding sources on building and sustaining capabilities. The THIRA and SPR are interconnected processes that, together, communities use to evaluate their preparedness. The THIRA/SPR sets a strategic foundation for putting the National Preparedness System into action. Communities complete the THIRA every three years and use the data from the process to assess their capabilities in the SPR, which is an annual review. It is important that communities complete the THIRA on a multi-year cycle, as it enables them to assess year-over-year trends in changes to their capabilities, while still periodically reviewing the capability targets to keep them relevant. All states and UASI funded Urban Areas are required to complete a THIRA every three years and an annual update to their SPR.

HSGP eligibility and the amount of funding allotted for each state, territory, or high-risk urban area is based on legislative authority and the fiscal year appropriation amount. The NOFO outlines funding allocations for each state, territory, and high-risk urban area. While FEMA

requires HSGP grant recipients to tie grant investments to support closing capability gaps or sustaining capabilities identified in the SPR, the THIRA/SPR is not a factor in determining funding allocations.

Building and Sustaining Capabilities

Subrecipients must prioritize grant funding for building and sustaining capabilities in areas that align with national priorities in the FY 2022 HSGP NOFO and capability gaps identified through the THIRA and SPR process. All capabilities being built or sustained must have a clear linkage to one or more core capabilities in the NPG.

Nationwide Cybersecurity Review

The cybersecurity of our Nation's critical infrastructure is a top priority. National preparedness, and more specifically the protection of critical infrastructure, requires an ability to prevent and respond to cyber incidents.

All subrecipients will be required to complete the 2022 Nationwide Cybersecurity Review (NCSR). The NCSR is estimated to be open from October 2022 to February 2023. The NCSR provides an avenue for agencies to benchmark and measure progress of improving their cybersecurity posture. The Chief Information Officer, Chief Information Security Officer, or equivalent for each subrecipient should complete the assessment. The NCSR is available at no cost and takes about 2-3 hours to complete.

Environmental Planning and Historic Preservation (EHP) Compliance

FEMA is required to consider the effects of its actions on the environment and/or historic properties to ensure that all activities and programs funded by the agency, including grant-funded projects, comply with Federal EHP regulations, laws, and Executive Orders, as applicable.

THE EHP REVIEW PROCESS MUST BE COMPLETED PRIOR TO INITIATING WORK ON A PROJECT. FEMA WILL NOT FUND PROJECTS THAT ARE INITIATED WITHOUT THE REQUIRED EHP REVIEW APPROVAL.

Subrecipients proposing projects that have the potential to impact the environment must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description that explains the goals and objectives of the proposed project along with supporting documentation so that FEMA may determine whether the proposed project has the potential to impact environmental resources and/or historic properties. In some cases, FEMA is also required to consult with other regulatory agencies and the public to complete the review process.

Subrecipients shall not undertake any project without the prior approval of GPD and must comply with all conditions placed on the project as the result of the EHP review. Any change to the approved project description will require re-evaluation for compliance with EHP requirements. Proposed construction or renovation projects that are part of larger projects funded from a non-FEMA source (such as an Emergency Operations Center that is part of a larger proposed public safety complex), also require that a FEMA EHP review be completed before the larger project is initiated. Activities that require an EHP review include but are not limited to construction and renovation projects, including certain installation activities; various equipment purchases such as sonar; and select training and exercise activities.

Failure of the subrecipient to meet EHP requirements, obtain required permits, and comply with any conditions that may be placed on the project as the result of FEMA's EHP review,

will result in the denial of Federal funding. The EHP screening memo must be submitted to FEMA, and the EHP review of the project must be completed, and approval received before funds are released to carry out the proposed project. Any project initiated prior to receiving EHP approval will result in a non-compliance finding and will not be eligible for funding.

For questions concerning applicability of any specific project or activity to the EHP Program, or for assistance with completing the required Environmental and Historic Preservation Screening Memo, please contact EMD_HSGP@michigan.gov.

Additionally, all subrecipients are required to comply with FEMA EHP Policy Guidance, FEMA Policy #108-023-1. Find the EHP screening memo at: [Grant Forms \(michigan.gov\)](#), and further EHP guidance can be found at [FEMA EHP Directive and Instructions](#).

Emergency Operations Plans (EOP)

Subrecipients should develop, maintain, or revise as necessary, jurisdiction-wide, all threats and hazards EOPs consistent with the Comprehensive Preparedness Guide (CPG) 101 Version 2.0, Developing and Maintaining Emergency Operations Plans. CPG 101 v.2 serves as the foundation for State, local, Tribal, and Territory emergency planning.

Ensuring the Protection of Civil Rights

As the Nation works towards achieving the NPG, it is important to continue to protect the civil rights of individuals. Subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations. Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS/FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from DHS/FEMA. The DHS Standard Terms and Conditions include a complete list of civil rights provisions that apply to subrecipients. The terms and conditions can be found at [DHS Standard Terms and Conditions](#). Additional information on civil rights provisions is available at [DHS Office of Equal Rights](#).

Prohibitions on Expending Grant or Cooperative Agreement Funds for Certain Telecommunications and Video Surveillance Services or Equipment.

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.326, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons. For additional guidance, please refer to FEMA Policy #405-143-1, Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim).

Additional information is provided on pages 30-32 of the FY 2022 HSGP NOFO.

Whole Community Engagement

Whole Community is a means by which residents, emergency management practitioners, organizational and community leaders, and government officials can collectively understand and assess the needs of their respective communities and determine the best ways to organize and

strengthen their assets, capacities, and interests. By doing so, a more effective path to societal security and resilience is built. SHSP and UASI subrecipients must engage with the Whole Community to advance community and individual preparedness and work as a nation to build and sustain resilience. Subrecipients must also integrate the needs of children, older adults, individuals with disabilities, individuals with limited English proficiency and others with access and functional needs, socio-economic factors, and cultural diversity with SHSP and UASI funds.

Collaboration with Tribes

Subrecipients are strongly encouraged to work with Tribal nations in overall initiatives such as whole community preparedness and emergency management planning.

Collaboration with Nonprofit Organizations

SHSP and UASI subrecipients are encouraged to work with the nonprofit community to address terrorism and all-hazards prevention concerns, seek input on the needs of the nonprofit sector, and support the goals of their investments.

Fusion Centers

A critical component of the national response to the 9/11 terrorist attacks was the development of a national-level, decentralized, and coordinated terrorism-related information sharing environment (ISE). State and local governments, supported by federal investments from DHS, the Department of Justice (DOJ), Department of Health and Human Services (HHS), and other federal agencies, established the National Network of Fusion Centers (National Network), which became the backbone of the national ISE.

Today's threats—including terrorism, drugs, active shooters, targeted violence, transnational organized crime, and cyber—require federal, state, and local governments to leverage this national capacity to effectively respond to the evolving nature of the various national and homeland security threats confronting our Nation. Ultimately, timely analysis of key indicators from local, state, and federal partners will enable all stakeholders to identify emerging threats and develop and implement data-driven strategies to prevent, protect against, and respond effectively.

To underscore the importance of the National Network as a critical component of our Nation's distributed homeland security and counterterrorism architecture, fusion centers **must** prioritize the following capabilities to further enable and mature this national asset:

- **Addressing Threats:** Fusion centers provide a national-level, decentralized, and coordinated ISE across all levels of government and disciplines that can be leveraged and applied to address threats to homeland security, national security, public safety, and/or public health, and especially those threats that may have little or no warning. Fusion centers should leverage and build upon their terrorism-focused analytic and information-sharing capabilities so they can be applied to address threats across the DHS mission space, including threats from both international terrorism and domestic violent extremists, threats to life and targeted violence, transnational organized criminal activity, cyber threats, and natural hazards, among others that require close collaboration with DHS operational, investigative, and analytic entities such as CBP, ICE, United States Secret Service (USSS), Cybersecurity and Infrastructure Security Agency (CISA), the United States Coast Guard (USCG), and FEMA.
- **Analytic Capability:** Fusion centers must maintain a strong analytic capability at tactical and strategic levels to address a wide array of threats or hazards that could have

implications for homeland security or national security. This capability includes, but is not limited to:

- Building and sustaining a capable workforce of analysts who have the necessary experience and training; access to open source, unclassified and classified information, products, data, suspicious activity reporting; tips/leads and online/social media-based threats; as well as necessary services and technology to facilitate analytic capabilities and collaboration.
- Assessing, evaluating, and deconflicting acts of targeted violence, threats to life, and other criminal or suspicious activity, to include potential indicators and behaviors, for potential connection to or implications for international or domestic terrorism, or other threats within the DHS mission space.
- Providing analytic support and responses to requests for information from federal, state, and local partners during no notice emerging threats, attacks, or incidents, as well as other planned events such as NSSEs.
- Conducting threat assessments within their respective jurisdictions, including the identification of threats, intelligence gaps, and mitigation efforts.
- Establishing, formalizing, and maintaining bi-directional information sharing with federal and other state agencies in accordance with jurisdictional authorities.
- Leveraging available resources and capabilities to conduct target and event deconfliction in support of threat identification, officer safety, and information sharing.
- Maintaining an ability to routinely support federal government efforts to watchlist terrorists and transnational organized crime actors.
- Appropriately planning for, and assessing/forecasting, prioritizing, and executing against both known and emerging threat vectors, and ensuring the safety and security of all operations, while protecting privacy, civil rights, and civil liberties.

Fusion centers should also consider their operational capacity when aligning manpower and resources in support of this capability (e.g., the ability to maintain watch and analytic support functions over a 24/7 operational tempo).

- **Technological Integration:** Access to data, information, and products is essential for fusion centers and the federal government. Just as threats do not stop at jurisdictional borders, fusion centers must be able to effectively access and share appropriate information and data across jurisdictions, agencies, and disciplines. Fusion centers must **ensure and certify via the Fusion Center Assessment** they have the necessary technological capacity to access, analyze, and share information, including criminal intelligence and online/social media threat information, both within their jurisdictions, as well as with other fusion centers across the country and with the Federal government.
- **Interagency Collaboration:** Fusion centers must maintain strong partnerships to enable operational, investigative, and analytic collaboration and deconfliction of threat information with other partners located within their jurisdiction and across their region, including HDTAs, RISS Centers, DHS intelligence and operational entities, FBI Field Offices, JTTFs, and major city/county intelligence units.

State and urban area fusion centers receiving SHSP or UASI grant funds will be evaluated based on compliance with the guidance and requirements for the National Network as set forth by DHS Intelligence and Analysis (I&A) through the annual Fusion Center Assessment.

Additional fusion center grant requirements are listed at <http://www.dhs.gov/homeland-security-grant-program-hsgp>. DHS/FEMA approved analyst courses that meet the grant requirement are listed at <http://www.dhs.gov/fema-approved-intelligence-analyst-training-courses>.

FY 2022 HSGP Funding Guidelines

Subrecipients must comply with all the requirements in 2 C.F.R. Part 200 (*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*).

Funding guidelines established within this section support the five mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and associated core capabilities within the NPG. Allowable investments made in support of the HSGP priorities as well as other capability-enhancing projects must have a nexus to terrorism preparedness and fall into the categories of planning, organization, equipment, training, or exercise. All funded projects must also support closing capability gaps or sustaining capabilities identified in the THIRA/SPR.

Multiple Purpose or Dual-Use of Funds

For both SHSP and UASI, many activities that support the achievement of core capabilities related to terrorism preparedness may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. However, all SHSP and UASI funded projects must assist subrecipients in achieving core capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

Planning (SHSP and UASI)

SHSP and UASI funds may be used for a range of emergency preparedness planning activities such as those associated with the development, review, and revision of the THIRA, SPR, continuity of operations plans, and other planning activities that support the NPG and placing an emphasis on updating and maintaining a current EOP that conforms to the guidelines outlined in CPG 101 v2.

Organization (SHSP and UASI)

Subrecipients must justify proposed expenditures of SHSP or UASI funds to support organization activities. Organizational activities include:

- Program management
- Development of whole community partnerships, through groups such as Citizen Corp Councils
- Structures and mechanisms for information sharing between the public and private sector
- Implementing models, programs, and workforce enhancement initiatives to address ideologically inspired radicalization to violence in the homeland
- Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors
- Operational Support
- Utilization of standardized resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident

- Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS) or needs resulting from a National Special Security Event
- Paying salaries and benefits for personnel to serve as qualified Intelligence Analysts. Per the *Personnel Reimbursement for Intelligence Cooperation and Enhancement (PRICE) of Homeland Security Act*, Pub. L. No. 110-412, § 2, codified in relevant part, as amended, at 6 U.S.C. § 609(a), SHSP and UASI funds may be used to hire new staff and/or contractor positions to serve as intelligence analysts to enable information/intelligence sharing capabilities, as well as support existing intelligence analysts previously covered by SHSP or UASI funding. See 6 U.S.C. § 609(a). To be hired as an intelligence analyst, staff and/or contractor personnel must meet at least one of the following criteria:

Complete training to ensure baseline proficiency in intelligence analysis and production within six months of being hired; and/or,

Previously served as an intelligence analyst for a minimum of two years either in a federal intelligence agency, the military, or state and/or local law enforcement intelligence unit.

- All fusion center analytical personnel must demonstrate qualifications that meet or exceed competencies identified in the Common Competencies for state, local, and tribal Intelligence Analysts, which outlines the minimum categories of training needed for intelligence analysts. A certificate of completion of such training must be on file with the State Administrative Agency (SAA).
- Migrating online services to the “.gov” internet domain.

Subrecipients may use up to 50 percent of their SHSP funding, and all high-risk urban areas may use up to 50 percent of their UASI funding, for personnel costs. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for allowable activities within the scope of the grant. Personnel expenses may include but are not limited to training and exercise coordinators, program managers and planners, intelligence analysts, and Statewide Interoperability Coordinators.

Organizational activities under SHSP and UASI include:

Operational Overtime Costs

In support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism, operational overtime costs are allowable for increased protective security measures at critical infrastructure sites or other high-risk locations and to enhance public safety during mass gatherings and high-profile events. In that regard, HSGP subrecipients are urged to consider using grant funding to support soft target preparedness activities. SHSP or UASI funds may be used to support select operational expenses associated with increased security measures in the authorized categories cited in the table below. FEMA retains the discretion to approve other types of requests that do not fit within one of the categories of the table.

Category		Description
1	National Terrorism Advisory System (NTAS)	Security measures in response to an increase in the threat level under the NTAS to an “elevated” or “imminent” alert status. GPD Information Bulletin No. 367, <i>Impact of National Terrorism Advisory System on</i>

		<i>Homeland Security Grant Programs</i> , remains applicable.
2	National Security Special Event (NSSE)	Security measures for a designated NSSE. NSSEs are events of national or international significance deemed by DHS to be a potential target for terrorism or other criminal activity.
3	Special Event Assessment Rating (SEAR) Level 1 through Level 4 Events	<p>Security measures required for SEAR Level 1 through Level 4 events as designated by the Department of Homeland Security (DHS) and included in the DHS National Special Events List, as defined below:</p> <ul style="list-style-type: none"> • SEAR 1: A significant event with national and/or international importance that may require extensive Federal interagency support; • SEAR 2: A significant event with national and/or international importance that may require some level of Federal interagency support. • SEAR 3: An event of national and/or international importance that requires only limited Federal support. • SEAR 4: An event with limited national importance that is managed at state and local level. <p>NOTE: In cases where a threat of terrorism can be associated with a SEAR Level 5 event, the event planners should coordinate with their state or territory Homeland Security Advisor to seek re-adjudication of the SEAR rating. Operational overtime for security measures associated with such events will be considered for approval by FEMA if re-adjudication results in a SEAR 1 through 4 rating.</p>
4	States of Emergency	Declarations of states of emergency by the Governor associated with a terrorism-related threat or incident . This excludes Presidentially declared major disasters or emergencies where Federal funding support for the proposed grant-funded activity is made available through the FEMA Public Assistance program or other Federal disaster grants.
5	National Critical Infrastructure Prioritization Program (NCIPP)	Protection of Level 1 and Level 2 facilities identified through the Department of Homeland Security's NCIPP based on a terrorism-related threat to critical infrastructure.
6	Directed Transit Patrols	Targeted security patrols in airports and major transit hubs based on a terrorism-related threat to transportation systems.

7	Other Related Personnel Overtime Costs	Overtime costs may be authorized for personnel assigned to directly support any of the security activities relating to the categories above. Examples include firefighters and emergency medical services personnel; public works employees who may be responsible for installing protective barriers and fencing; public safety personnel assigned to assist with event access and crowd control; emergency communications specialists; fusion center analysts; National Guard; contract security services; etc.
8	Operational Support to a Federal Agency	Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities related to homeland security/terrorism preparedness and specifically requested by a federal agency. Allowable costs are limited to overtime associated with Federally requested participation in eligible activities, including anti-terrorism task forces, Joint Terrorism Task Forces (JTTFs), Area Maritime Security Committees (as required by the Maritime Transportation Security Act of 2002), DHS Border Enforcement Security Task Forces, and Integrated Border Enforcement Teams. In addition, reimbursement for operational overtime law enforcement activities related to combating transnational crime organizations in support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism is an allowable expense under SHSP and UASI on a case-by-case basis. Grant funding can only be used in proportion to the Federal man-hour estimate and only after funding for these activities from other Federal sources (i.e., FBI JTTF payments to state and local agencies) has been exhausted.

All allowable operational overtime costs are also subject to the administration requirements outlined in the following subsection.

Administration of Operational Overtime Requests:

- Except for an elevated National Security Special Event alert, SHSP or UASI funds may only be spent for operational overtime costs upon prior written approval by FEMA. FEMA will consider requests for special event activities up to one year in advance. However, such requests must be within the award's current period of performance and must not result in the need for a request to extend the period of performance.
- All operational overtime requests must clearly explain how the request meets the criteria of one or more of the categories listed in the table above. Requests must address the threat environment as it relates to the event or activity requiring operational overtime support and explain how the overtime activity is responsive to the threat.

- Post-event operational overtime requests will only be considered on a case-by-case basis, where it is demonstrated that exigent circumstances prevented submission of a request in advance of the event or activity.
- Under no circumstances may FEMA grant funding be used to pay for costs already supported by funding from another federal source.
- FEMA will consult and coordinate with appropriate DHS components as necessary to verify information used to support operational overtime requests.

Personnel Costs

Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable HSGP planning, training, exercise, and equipment activities. Personnel may include but are not limited to training and exercise coordinators, program managers for activities directly associated with SHSP and UASI funded activities, intelligence analysts, and Statewide Interoperability Coordinators.

For further details, refer to Information Bulletin No. 421, Clarification on the Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act of 2008 (Public Law 110–412 – the PRICE Act), Aug. 22, 2017, or contact the MSP/EMHSD.

HSGP funds may not be used to support the hiring of any personnel to fulfil traditional public health and safety duties nor to supplant traditional public health and safety positions and responsibilities.

The following definitions apply to personnel costs:

- *Hiring.* State and local entities may use grant funding to cover the salary of newly hired personnel who are exclusively undertaking allowable FEMA grant activities as specified in this guidance. This may not include new personnel who are hired to fulfill any non-FEMA program activities under any circumstances. Hiring will always result in a net increase of Full Time Equivalent employees.
- *Overtime.* These expenses are limited to the additional costs that result from personnel working over and above 40 hours of weekly work time as the direct result of their performance of FEMA-approved activities specified in this guidance. Overtime associated with any other activity is not eligible.
- *Backfill-Related Overtime.* Also called “Overtime as Backfill,” these expenses are limited to overtime costs that result from personnel who are working overtime (as identified above) to perform the duties of other personnel who are temporarily assigned to FEMA-approved activities outside their core responsibilities. Neither overtime nor backfill expenses are the result of an increase of FTE employees.
- *Supplanting.* Grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Subrecipients may be required to supply documentation certifying that a reduction in non-federal resources occurred for reasons other than the receipt or expected receipt of federal funds.

Equipment (SHSP and UASI)

The 21-allowable prevention, protection, mitigation, response, and recovery equipment categories for HSGP are listed on the Authorized Equipment List (AEL). The AEL is available at <http://www.fema.gov/authorized-equipment-list>. Some equipment items require prior approval from FEMA before obligation or purchase of the items. Please reference the grant

notes for each equipment item to ensure prior approval is not required or to ensure prior approval is obtained if necessary.

Unless otherwise stated, all equipment must meet all mandatory regulatory and/or FEMA-adopted standards to be eligible for purchase using these funds. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance. Such investments must be coordinated with the Statewide Interoperability Coordinators, and the State Interoperability Governing Body to ensure interoperability and long-term compatibility.

Grant funds may be used for the procurement of medical countermeasures. Procurement of medical countermeasures must be conducted in collaboration with state, city, or local health departments that administer federal funds from Health and Human Services for this purpose and with existing Metropolitan Medical Response System committees where available, to sustain their long-term planning for appropriate, rapid, and local medical countermeasures, including antibiotics and antidotes for nerve agents, cyanide, and other toxins. Procurement must have a sound threat-based justification with an aim to reduce the consequences of mass casualty incidents during the first crucial hours of a response. Prior to procuring pharmaceuticals, subrecipients must have in place an inventory management plan to avoid large periodic variations in supplies due to coinciding purchase and expiration dates. Subrecipients are encouraged to enter into rotational procurement agreements with vendors and distributors. Purchases of pharmaceuticals must include a budget for the disposal of expired drugs within each fiscal year's Period of Performance (PoP) for HSGP. The cost of disposal cannot be carried over to another FEMA grant or grant period.

Emergency Medical Services electronic patient care data systems should comply with the most current data standard of the National Emergency Medical Services Information System (www.NEMSIS.org).

Requirements for Small Unmanned Aircraft System (SHSP, UASI, and OPSG)

All requests to purchase Small Unmanned Aircraft Systems with FEMA grant funding must comply with Information Bulletin (IB) 426 and IB 438 and include a description of the policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties of the jurisdiction that will purchase, take title to, or otherwise use the equipment.

Acquisition and Use of Technology to Mitigate UAS (Counter-UAS)

In August 2020, FEMA was alerted of an advisory guidance document issued by DHS, the Department of Justice, the Federal Aviation Administration, and the Federal Communications Commission: <https://www.dhs.gov/publication/interagency-legal-advisory-uas-detection-and-mitigation-technologies>. The purpose of the advisory guidance document is to help non-federal public and private entities better understand the federal laws and regulations that may apply to the use of capabilities to detect and mitigate threats posed by UAS operations (i.e., Counter-UAS or C-UAS). The Departments and Agencies issuing the advisory guidance document, and FEMA, do not have the authority to approve non-federal public or private use of UAS detection or mitigation capabilities, nor do they conduct legal reviews of commercially available product compliance with those laws. The advisory does not address state and local laws nor potential civil liability, which UAS detection and mitigation capabilities may also implicate. It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection and/or

mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation system and should not rely solely on vendors' representations of the systems' legality or functionality. Please also see the DHS press release on this topic for further information: [Interagency Issues Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems | Homeland Security \(dhs.gov\)](#).

Training (SHSP and UASI)

Allowable training-related costs under the HSGP include the establishment, support, conduct, and attendance of training specifically identified under the SHSP and UASI program and/or in conjunction with emergency preparedness training by other federal agencies (e.g., Health and Human Services and Department of Transportation). Training conducted using HSGP funds should address a performance gap identified through a training and exercise plan or other assessments (e.g., National Emergency Communications Plan Goal Assessments) and contribute to building a capability that will be evaluated through a formal exercise. Any training or training gaps, including training related to under-represented diverse populations that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations, should be identified in a training and exercise plan and addressed in the state or high-risk urban area training cycle.

Subrecipients are encouraged to use existing training rather than developing new courses. When developing new courses, subrecipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate model of instructional design. Subrecipients are also encouraged to utilize the National Training and Education Division's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by DHS/FEMA/National Training and Education Division. This includes the Center for Domestic Preparedness, the Emergency Management Institute, and the National Training and Education Division's Training Partner Programs, including the Continuing Training Grants, the National Domestic Preparedness Consortium, the Rural Domestic Preparedness Consortium, and other partners.

The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, territorial, and tribal audiences. All courses have been approved through the National Training and Education Division's course review and approval process. The catalog can be accessed at <http://www.firstrespondertraining.gov>.

Exercises (SHSP and UASI)

Exercises conducted with grant funding should be managed and conducted consistent with The Homeland Security Exercise and Evaluation Program. The guidance for exercise design, development, conduct, evaluation, and improvement planning is located at <https://www.fema.gov/emergency-managers/national-preparedness/exercises>.

Maintenance and Sustainment (SHSP, UASI, and OPSG)

Preparedness grant funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees. These contracts may only exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment and as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance

contract on an already-owned piece of equipment or system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with HSGP funds or for equipment dedicated for HSGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

The use of FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable under all active and future grant awards, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the POP of the specific grant funds used to purchase the plan or warranty.

Grant funds are intended to support the Goal by funding projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in FEMA's IB 379, Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding, initially for FY 2007-2011, allows for the expansion of eligible maintenance and sustainment costs which must be in (1) direct support of existing capabilities; (2) must be an otherwise allowable expenditure under the applicable grant program; (3) be tied to one of the core capabilities in the five mission areas contained within the Goal, and (4) shareable through the EMAC. Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant or any other source of funding other than FEMA preparedness grant program dollars.

Law Enforcement Terrorism Prevention Activities Allowable Costs (SHSP and UASI)

Activities eligible for the use of LETPA focused funds include but are not limited to:

- Maturation, enhancement, and sustainment of designated state and major urban area fusion centers, including information sharing and analysis, threat recognition, terrorist interdiction, and training/ hiring of intelligence analysts;
- Coordination between fusion centers and other intelligence, operational, analytic, or investigative efforts including, but not limited to JTTFs, Field Intelligence Groups (FIGs), High-Intensity Drug Trafficking Areas (HIDTA), Regional Information Sharing Systems (RISS) Centers, criminal intelligence units, real-time crime analysis centers and DHS intelligence, operational, analytic, and investigative entities;
- Implementation and maintenance of the nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), including training for front-line personnel on identifying and reporting suspicious activities, tips/leads, and online/social media-based threats, as well as the execution and management of threat assessment programs to identify, evaluate, and analyze indicators and behaviors indicative of terrorism, targeted violence, threats to life, and other criminal activity;
- Management and operation of activities that support the execution of the intelligence process and fusion centers, including but not limited to: Fusion Liaison Officer (FLO) programs, security programs to protect the facility, personnel, and information, and the protection of privacy, civil rights, and civil liberties;
- Implementation of the "If You See Something, Say Something®" campaign to raise public awareness of indicators of terrorism and terrorism-related crime and associated

efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS “If You See Something, Say Something®” campaign using grant funds work directly with the DHS Office of Partnership and Engagement (OPE) to ensure all public awareness materials are consistent with DHS’s messaging and strategy for the campaign and compliant with the initiative’s trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the Campaign’s Office (seesay@hq.dhs.gov), must be facilitated by the FEMA HQ Preparedness Officer;

- Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical infrastructure sites or at-risk nonprofit organizations;
- Building and sustaining preventive radiological and nuclear detection capabilities, including those developed through the Securing the Cities initiative; and
- Integration and interoperability of systems and data, such as computer aided dispatch and record management systems, to facilitate the collection, evaluation, and assessment of suspicious activity reports, tips/leads, and online/social media-based threats.

Construction and Renovation (SHSP and UASI)

Project construction using SHSP and UASI funds may not exceed the greater of \$1,000,000 or 15 percent of the grant award. For the purposes of the limitations on funding levels, communications towers are not considered construction. See guidance on communication towers below.

Written approval must be provided by FEMA prior to the use of any HSGP funds for construction or renovation. When applying for construction funds, subrecipients must submit evidence of approved zoning ordinances, architectural plans, and any other locally required planning permits. Additionally, subrecipients are required to submit a SF-424C form with budget detail citing the project costs.

Subrecipients using funds for construction projects must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). subrecipients must ensure that their contractors or subcontractors for construction projects pay workers no less than the prevailing wages for laborers and mechanics employed on projects of a character like the contract work in the civil subdivision of the State in which the work is to be performed. Additional information regarding compliance with the *Davis-Bacon Act*, including Department of Labor wage determinations, is available online at <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Western Hemispheric Travel Initiative (SHSP)

In addition to the expenditures outlined above, SHSP funds may be used to support the implementation activities associated with the Western Hemisphere Travel Initiative (WHTI), including the issuance of WHTI-compliant tribal identification cards.

28 CFR Part 23 Guidance

FEMA requires that any information technology system funded or supported by these funds comply with 28 CFR, Part 23, Criminal Intelligence Systems Operating Policies if this regulation is determined to be applicable.

Unallowable Costs (SHSP, UASI, and OPSG):

- Per FEMA policy, the purchase of weapons and weapons accessories, including ammunition, is not allowed with HSGP funds.
- Grant funds may not be used for the purchase of equipment not approved by FEMA. Grant funds must comply with IB 426 and may not be used for the purchase of the following equipment: firearms; ammunition; grenade launchers; bayonets; or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.
- Unauthorized exercise-related costs include:
 - Reimbursement for the maintenance or wear and tear costs of general use vehicles, medical supplies, and emergency response apparatus.
 - Equipment that is purchased for permanent installation and/or use, beyond the scope of the conclusion of the exercise.

FY 2022 HSGP-SHSP Investments

The Michigan FY 2022 HSGP-SHSP Investment Justification is comprised of multiple investments designed to enhance statewide capabilities in specific core areas, in alignment with Federal and statewide initiatives.

Stakeholder Preparedness Review Alignment

The FY 2022 SHSP investments are derived from specific capability shortfalls identified through the annual THIRA and SPR process.

The THIRA is a three-step risk assessment completed every three years. It helps communities answer the following questions:

- What threats and hazards can affect our community?
- If they occurred, what impacts would those threats and hazards have on our community?
- Based on those impacts, what capabilities should our community have?

The THIRA helps communities understand their risks and determine the level of capability they need to address those risks. The outputs from this process lay the foundation for determining a community's capability gaps during the SPR process. The FY 2022 SHSP investment descriptions are based upon the functional gaps identified in the SPR.

HSGP Project Workbook:

The HSGP project workbooks are designed to establish a link between subrecipient investment projects, investment descriptions, and the THIRA and SPR. Subrecipients must identify specific functional areas where capability gaps exist that will be addressed by their projects, based upon the core capability that the project supports. Establishing this link will validate investment alignment as well as alignment to the THIRA and SPR. Functional areas where capability gaps exist within each core capability are provided in Appendix C of this document. An example of a project description which identifies the applicable core capability functional gap(s) is provided below. Please refer to the FY 2022 HSGP project workbook instructions for additional information.

HSGP PROJECT DESCRIPTION EXAMPLE:

Project Title: Critical Infrastructure and Key Resource (CIKR) Resilience

Core Capability: Physical Protective Measures

This project will continue to identify and prioritize key critical infrastructure sites and conduct vulnerability assessments. The assessments are an ongoing initiative to evaluate the top 10 CIKR sites in the region and identify the most effective means of hardening the facilities or infrastructure. Completion of the assessments is anticipated within this calendar year; however, FY 2022 funds will also be used to implement physical protective measures and provide training for CIKR security staff. Public outreach may also be conducted to educate the public and encourage reporting of suspicious activities in or around CIKR sites. This project addresses functional areas where capability gaps exist, as identified in the SPR, including: identifying and

prioritizing assets to protect; physical security measures; and site-specific and process-specific risk assessments.

Supported Functional Areas Where Capability Gaps Exist:

- Identifying and prioritizing assets to protect
- Physical security measures
- Site-specific and process-specific risk assessments

The FY 2022 Michigan HSGP – SHSP Investments include:

1. Michigan Cybersecurity (NPA)
2. Protection of Soft Targets and Crowded Places (Required NPA)
3. Intelligence and Information Sharing (Required NPA)
4. Combating Domestic Violent Extremism (Required NPA)
5. Community Preparedness and Resilience (Required NPA)
6. Election Security (NPA)
7. Homeland Security Planning
8. Operational Preparedness and Response
9. Terrorism Prevention and Protection
10. CBRNE Response and Recovery

The FY 2022 HSGP funding must be utilized to build and sustain core capabilities within the NPG. In addition, all projects must be aligned with capability targets and gaps identified through the THIRA/SPR process.

Specialized Response Assets: All Regions are expected to sustain the capabilities of specialized response assets such as the Regional Response Team Network and Search and Rescue teams and capabilities. Support should be provided through appropriate planning, equipment, training, and exercise activities.

Important: When making SHSP and UASI expenditures, they must be consistent with the investment descriptions included in the FY 2022 SHSP or UASI Investment Justification, respectively. All investment expenditures must also be included in the subrecipient project workbooks. Before any SHSP and UASI expenditures can be made, all individual solution area costs must be reviewed and approved by MSP/EMHSD via the Alignment and Allowability Form (AAF). The FY 2022 HSGP - UASI Investment Justification is available to the Southeast Michigan UASI Region through the regional fiduciary or MSP/EMHSD.

Note: Investments 1-6 above are specific to the national priority area funding requirements. Investments 2-5 are each required to be funded.

Investment # 1: Michigan Cybersecurity

Core Capabilities:

- Cybersecurity
- Intelligence and information sharing
- Planning
- Public information and warning
- Operational coordination
- Screening, search, and detection
- Access control and identity verification
- Supply chain integrity and security
- Risk management for protection programs and activities
- Long-term vulnerability reduction
- Situational assessment
- Infrastructure systems
- Operational communications

Investment Description:

Because the threat of a cyberattack is always persistent, Michigan places a high priority on cybersecurity. Although significant investments have been made in cybersecurity, cyberattacks continue to cause damage to companies, governments, and individuals. Developing and improving capabilities to protect sensitive data, personally identifiable information, protected health information, personal information, intellectual property, and government and industry information systems is critical. This investment addresses gaps identified in the 2021 Stakeholder Preparedness Review to mitigate the risk of attacks to Michigan's cyber infrastructure. Functional areas where gaps were identified for Cybersecurity include: guidelines, regulations, and standards; sharing threat information; updating cyber plans; controlling electronic access; protective measures; detecting malicious activities; securing CIKR and SCADA systems; technical countermeasures; continuity of operations for cyber systems; investigating malicious actors; and end user awareness. Michigan identified gaps across all solution areas in each functional area of the Cybersecurity core capability. The SPR also identified more specific needs such as personnel to conduct cyber assessments and continuing and expanding current training and exercise efforts. Cyber-related gaps were also identified in 2021 or previous years in the following core capabilities: Intelligence and Information Sharing; Planning; Public Information and Warning; Operational Coordination; Screening, Search, and Detection; Access Control and Identity Verification; Supply Chain Integrity and Security; Risk Management for Protection Programs and Activities; Long- Term Vulnerability Reduction; Situational Assessment; Infrastructure Systems; and Operational Communications. Michigan maintains a robust cybersecurity program; however, cyber threats continuously evolve, and public and private sector partners remain vulnerable. Cybersecurity is a high priority core capability and with the increasing threat of cyberattacks, cybersecurity will remain a top priority in Michigan.

Investment # 2: Enhancing the Protection of Soft Targets and Crowded Places

Core Capabilities:

- Operational coordination
- Public information and warning
- Intelligence and information sharing
- Interdiction and disruption
- Screening, search, and detection
- Access control and identify verification
- Physical protective measures
- Risk management for protection programs and activities

Investment Description:

Soft targets across the nation face increasing threats from potential acts of terrorism and active assailants, and Michigan is no exception. Locations that are easily accessible to the public and maintain minimal security are particularly vulnerable due to the relative ease with which an adversary can access and surveil potential targets and the myriad of simple tactics that can be used to carry out attacks, such as small arms, Improvised Explosive Devices, edged weapons, and vehicle ramming. To address this threat, Michigan will support multiple core capability gaps identified in the 2021 SPR, or earlier versions if the capability was not assessed in 2021. Gaps in Interdiction and Disruption include: interdicting cargo, conveyances, and persons, anti-terrorism operations; border security; CBRNE detection; CBRNE render safe; deterrent law enforcement presence; tactical law enforcement operations; tracking and targeting terrorists and their weapons; wide-area search and detection; financial disruption; and preventing acquisition of CBRNE. Functional gaps in Screening, Search and Detection include: screening, wide-area search, electronic search; explosives detection; locating terrorists; physical investigation; wide-area search; promoting an observant nation; radiological and nuclear detection; bio-surveillance; CBRNE detection; chemical and biological detection, and laboratory testing. The functional shortfalls in Physical Protective Measures to be addressed include: biosecurity; border protection; identifying and prioritizing assets to protect; site-specific and process specific risk assessments; and physical security measures. Gaps in Risk Management for Protection Programs and Activities include: analysis tools; data collection; incorporating risk assessments in exercise design; risk assessment; risk communication; and risk management planning. Other core capabilities that may be addressed include: Access Control and Identity Verification; Intelligence and Information Sharing; Public Information and Warning and Operational Coordination. These investments will help to lessen the risk of an attack on soft target venues such as shopping centers, and other areas of gatherings, as well as the impact of an attack, should one occur.

Investment # 3: Intelligence and Information Sharing

Core Capabilities:

- Intelligence and information sharing
- Interdiction and disruption
- Planning
- Public information and warning
- Operational coordination
- Risk management for protection

Investment Description:

This investment will allow Michigan to sustain the primary fusion center, the Michigan Intelligence Operations Center (MIOC), support the Detroit Southeast Michigan Intelligence Information Center (DSEMIIC), and continue to address functional area shortfalls related to the Intelligence and Information Sharing capability identified in the 2021 SPR. The functional area shortfalls include: establishing intelligence and information requirements; analysis of intelligence and information; continuous threat assessment; safeguarding sensitive information; developing reports and products; disseminating intelligence and information; exploiting and processing information; feedback and evaluation; gathering intelligence; monitoring information; and establishing information requirements. There are also functional area shortfalls in Interdiction and Disruption that will be addressed which include: anti-terrorism operations; border security; CBRNE detection; CBRNE render safe; deterrent law enforcement presence; tactical law enforcement operations; tracking and targeting terrorists and their weapons; wide area search and detection; interdicting cargo, conveyances, and persons; financial disruption, and preventing acquisition of CBRNE. The SPR also identified a need for technology upgrades and fusion liaisons in Michigan regions. Additional core capabilities that may be addressed include: Planning; Public Information and Warning; Operational Coordination; and Risk Management for Protection programs and activities. Activities supported by this investment are a priority because it will support the four Critical Operational Capabilities (COCs) for fusion centers (COC 1, Receive; COC 2, Analyze; COC 3, Disseminate; and COC 4, Gather) and will improve Michigan's information sharing environment to include local, state, and federal agencies.

Investment # 4: Combating Domestic Violent Extremism**Core Capabilities:**

- Interdiction and disruption
- Screening, search, and detection
- Physical protective measures
- Intelligence and information sharing
- Planning
- Public information and warning
- Operational coordination
- Risk management for protection programs and activities

Investment Description:

The nation faces an increasingly complex and evolving threat of domestic violent extremism. State and local responders must continuously build capabilities necessary to prepare for a diverse range of threats. To prepare the state against domestic violent extremism Michigan will focus on strengthening shortfalls identified in the SPR in a variety of core capabilities. Gaps identified for Interdiction and Disruption include: anti-terrorism operations; border security; CBRNE detection; CBRNE render safe; deterrent law enforcement presence; tactical law enforcement operations; tracking and targeting terrorists and their weapons; wide-area search and detection; interdicting cargo, conveyances, and persons; financial disruption, and preventing acquisition of CBRNE. Shortfalls identified in Screening, Search and Detection include: screening, wide-area search, electronic search; explosives detection; locating terrorists; physical investigation; wide-area search; promoting an observant nation; radiological and nuclear detection; bio surveillance; CBRNE detection; chemical and biological detection, and laboratory testing. The functional area gaps in Physical Protective Measures include: biosecurity; border protection; identifying and prioritizing assets to protect; site-specific and

process specific risk assessments; and physical security measures. The functional area shortfalls for Intelligence and information sharing include: establishing intelligence and information requirements; analysis of intelligence and information; continuous threat assessment; safeguarding sensitive information; developing reports and products; disseminating intelligence and information; exploiting and processing information; feedback and evaluation; gathering intelligence; monitoring information; and establishing information requirements. Gaps in Risk Management for Protection Programs and Activities include: analysis tools; data collection; incorporating risk assessments in exercise design; risk assessment; risk communication; and risk management planning. Additional capabilities that may be addressed include: Planning; Public Information and Warning; and Operational Coordination. This investment will work towards closing these gaps and providing the resources necessary to prevent, protect against, and respond to domestic violent extremism being carried out in Michigan.

Investment # 5: Community Preparedness and Resilience

Core Capabilities:

- Planning
- Public information and warning
- Community resilience
- Risk management for protection programs and activities
- Mass care services
- Long-term vulnerability reduction

Investment Description:

The challenges faced by communities today are increasingly complex and both human-caused and natural disasters are becoming more frequent and costly. This investment sustains capabilities for community resilience and addresses gaps identified in Michigan's SPR. The Planning core capability may be supported through sustaining capabilities and addressing shortfalls in the following functional areas: Continuity planning; including individuals with disabilities or AFN; incorporating risk analyses; integrating different plans; pre-incident planning; strategic planning; evaluating and updating plans; operational planning; and whole community involvement and coordination. Gaps in Public Information and Warning include: delivering actionable guidance; alerts and warnings; culturally and linguistically appropriate messaging; inclusiveness of the entire public; developing standard operating procedures for public information; new communications tools and technologies; protecting sensitive information; public awareness campaigns; and traditional communications mechanisms. Community Resilience gaps include: understanding the community; and collaborative planning and decision making; communication and outreach; education and skill building; partnership building. Gaps in Risk Management for Protection Programs and Activities include: analysis tools; data collection; incorporating risk assessments in exercise design; risk assessment; risk communication; and risk management planning. Gaps in Mass Care Services include: sheltering; ensuring access; feeding; hydration; pets; resource distribution; family reunification; and relocation assistance. Risk and Disaster Resilience Assessment gaps include: modeling and analysis; obtaining and sharing data; education and training. Long-term Vulnerability Reduction gaps include: developing neighborhood civic organizations and individual family preparedness. Gaps identified in Intelligence and Information Sharing related to community resilience may also be addressed. This investment allows Michigan to close gaps and build preparedness while also promoting strong community systems.

Investment # 6: Election Security

Core Capabilities:

- **Cybersecurity**
- **Intelligence and information sharing**
- Planning
- Long-term vulnerability reduction
- Situational assessment
- Infrastructure systems
- Physical protective measures

Investment Description:

Free and fair elections play a vital role in our society. Securing election infrastructure against new and evolving threats, both cyber and physical, is fundamental to ensure the integrity of elections. Michigan will invest funds to build capabilities enabling state and local election officials to assess risk, secure systems, and respond to any cyber or physical attacks. This investment will implement physical security measures in support of the Physical Protective Measures core capability and may also support the Cybersecurity and Planning capabilities. Gaps Physical Protective Measures to be addressed include: biosecurity; border protection; identifying and prioritizing assets to protect; site-specific and process specific risk assessments; and physical security measures. Functional areas where gaps were identified for Cybersecurity include: guidelines, regulations, and standards; sharing threat information; updating cyber plans; controlling electronic access; protective measures; detecting malicious activities; securing CIKR and SCADA systems; technical countermeasures; continuity of operations for cyber systems; investigating malicious actors; and end user awareness. And Planning gaps include: continuity planning; including individuals with disabilities or AFN; incorporating risk analyses; integrating different plans; pre-incident planning; strategic planning; evaluating and updating plans; operational planning; and whole community involvement and coordination. The following additional core capabilities relating to election security may also be supported: Intelligence and Information Sharing; Long-term Vulnerability Reduction; Situational Assessment; and Infrastructure Systems. This investment will help Michigan manage risk to election security and combat and secure the state's physical and cyber infrastructure against new and evolving threats.

Investment # 7: Homeland Security Planning

Core Capabilities:

- Planning
- Long-term vulnerability reduction
- Risk and disaster resilience assessment
- Threats and hazard identification
- Risk management for protection programs and activities
- Supply chain integrity and security
- Housing
- Natural and cultural resources

Investment Description:

This investment supports the National Preparedness System through planning efforts designed to build and sustain Michigan's capacity to address threats and hazards facing whole

community members. The primary core capability addressed by this investment is Planning, where shortfalls were identified in the SPR. Additional core capabilities supported by this investment include: Long-term Vulnerability Reduction; Risk and Disaster Resilience Assessment; Threats and Hazards Identification; Housing, Natural and Cultural Resources, Risk Management for Protection Programs and Activities; and Supply Chain Integrity and Security. The Planning core capability is supported through sustaining capabilities and addressing shortfalls in the following functional areas: Continuity planning; including individuals with disabilities or AFN; incorporating risk analyses; integrating different plans; pre-incident planning; strategic planning; evaluating and updating plans; operational planning; and whole community involvement and coordination. Functional gaps in Threat and Hazards Identification include: data collection and sharing; estimating frequency and magnitude; modeling and analysis; stakeholder collaboration; and assess threats and hazards. Gaps in Risk and Disaster Resilience Assessment include: modeling and analysis; education and training; and obtaining and sharing data. Long-term Vulnerability Reduction gaps include: individual and family preparedness; developing neighborhood civic organizations. Housing gaps include: addressing housing shortages, accessibility, affordability, and assessments, and transition from interim to permanent/long-term housing. Natural and Cultural Resources gaps include: environmental and historic preservation and restoration. Gaps in Risk Management for Protection Programs and Activities include: analysis tools; data collection; incorporating risk assessments in exercise design; risk assessment; risk communication; and risk management planning. Finally, shortfalls in Supply Chain Integrity and Security include: analysis of supply chain dependencies; implementing countermeasures; implementing physical protection; integrating security processes; and verification and detection. Strengthening planning and preparedness activities is an essential component of protecting life, ensuring safety, and building resilient communities, making planning a high priority.

Investment # 8: Operational Preparedness and Response

Core Capabilities:

- Operational coordination
- Situational assessment
- Operational communications
- Infrastructure systems
- Logistics and supply chain management
- Critical transportation

Investment Description:

This investment will sustain existing and build new capabilities to improve competencies in operational preparedness and response and to achieve the capability targets established in the Threat and Hazard Identification and Risk Assessment (THIRA). Core capabilities that are addressed by this investment are Operational Coordination; Situational Assessment; Operational Communications; Infrastructure Systems, Logistics and Supply Chain Management and Critical Transportation. The SPR identified shortfalls in each of these core capabilities, making operational preparedness and response a high priority area. The functional area shortfalls in Operational Coordination include: allocating and mobilizing resources; EOC management; Ensuring COG and essential services; establishing roles and responsibilities, determining priorities, objectives, strategies; ensuring information flow; ensuring unity of effort; establishing a common operating picture; establishing lines of communication; command, control, and coordination; stakeholder engagement; NIMS/ICS compliance; unified and

coordinated operational structure. Functional area shortfalls in Situational Assessment include: analyzing information; assessing hazard impacts; tracking response activities; delivering situation reports; and stakeholder engagement. The Operational Communications gaps identified in Michigan's SPR include: interoperability between responders; communications between responders and the affected population; data communications; re-establishing communications infrastructure; re-establishing critical information networks; and voice communications. All communications investments will be P-25 compliant and align with Michigan's Statewide Communications Interoperability Plan. Finally, the following additional core capabilities may also be supported: Infrastructure Systems; Logistics and Supply Chain Management; and Critical Transportation. These core capabilities continue to be priorities and sustainment and enhancement is necessary to ensure Michigan maintains an effective operational preparedness and response capacity.

Investment # 9: Terrorism Prevention and Protection

Core Capabilities:

- Intelligence and information sharing
- Interdiction and disruption
- Screening, search, and detection
- Forensics and attribution
- Access control and identity verification
- Physical protective measures

Investment Description:

The Terrorism Prevention and Protection investment will strengthen and sustain Michigan's capabilities to prevent, avoid, or stop a threatened or actual act of terrorism, to include foreign and domestic threat actors, large-scale attacks, and threats posed by lone offenders or small groups. Michigan will focus on capability shortfalls identified in the 2021 SPR. Functional area shortfalls in Intelligence and Information Sharing include: establishing intelligence and information requirements; analysis of intelligence and information; continuous threat assessment; safeguarding sensitive information; developing reports and products; disseminating intelligence and information; exploiting and processing information; feedback and evaluation; gathering intelligence; monitoring information; and establishing information requirements. Gaps in Interdiction and Disruption include: anti-terrorism operations; border security; CBRNE detection; CBRNE render safe; deterrent law enforcement presence; tactical law enforcement operations; tracking and targeting terrorists and their weapons; wide-area search and detection; interdicting cargo, conveyances, and persons; financial disruption, and preventing acquisition of CBRNE. Screening, Search and Detection gaps: screening, wide-area search, electronic search; explosives detection; locating terrorists; physical investigation; wide-area search; promoting an observant nation; radiological and nuclear detection; bio-surveillance; CBRNE detection; chemical and biological detection, and laboratory testing. Forensics and Attribution gaps: assessing terrorist capabilities; CBRNE material analysis; crime scene preservation and exploitation; evidence collection; digital media and network exploitation; forensics analysis; and terrorist investigations. Capability shortfalls in Access Control and Identity Verification: controlling cyber access; controlling physical access; and verifying identity. Physical Protective Measures gaps: biosecurity; border protection; identifying and prioritizing assets to protect; site specific and process specific risk assessments; and physical security measures. This investment is a priority because it directly supports the Prevention mission area which is the only mission area specifically targeting prevention of an initial or follow-on attack,

making it a fundamental component of any counterterrorism effort. Activities in this investment may also support the protection mission area.

Investment # 10: CBRNE Response and Recovery

Core Capabilities:

- Environmental response/health and safety
- Mass search and rescue operations
- On-scene security, protection, and law enforcement
- Fire management and suppression
- Health and social services
- Economic recovery
- Public health, health care and Emergency Medical Services
- Fatality management

Investment Description:

This investment will allow Michigan to build and sustain response capabilities for chemical, biological, radiological, nuclear, or explosive (CBRNE) incidents. This investment will address specific functional gaps identified in the SPR in the following core capabilities: Environmental Response/Health and Safety; Mass Search and Rescue Operations; On-scene Security, Protection and Law Enforcement, Public Health, Healthcare, and Emergency Medical Services, Fatality Management Services, Fire Management and Suppression, Health and Social Services, and Economic Recovery. The functional area shortfalls in Environmental Response/Health and Safety include: decontamination; environmental impact analysis; predictive modeling; health and safety monitoring and assessment; responder safety; survivor safety and assistance; hazardous material clean up; debris removal. Functional shortfalls in Mass Search and Rescue to be addressed include: rescue operations; search operations; specialized operations; synchronizing operations; and community-based search and rescue. Functional area shortfalls in On-scene Security, Protection, and Law Enforcement that will be addressed include: protecting response personnel; securing disaster areas; and law enforcement. Gaps in Public Health, Healthcare and Emergency Medical Services include: triage and initial stabilization; emergency medical services; definitive care; clinical laboratory testing. Fatality Management Services gaps include: body recovery; mortuary services; victim identification; bereavement counseling; family reunification. Functional shortfalls in Fire Management and Suppression include: wildland firefighting; specialized firefighting; initial attack firefighting; extended attack firefighting; structural firefighting; and firefighting operations. Gaps in Health and Social Services include: healthcare facilities and coalitions; social services; behavioral health; ensuring access. Lastly, the Economic Recovery gaps include: reopening businesses; business/economic continuity planning; developing recovery objectives; developing the workforce; disseminating information; economic impact assessments; incentivizing entrepreneurial and business development; management planning. Each capability plays a crucial role in response to and/or recovery from CBRNE incidents or terrorism events and remain priorities in the state.

Appendix A: Summary of the National Preparedness Goal

The National Preparedness Goal (NPG) is “[a] secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.” The NPG essentially defines what it means for all communities to be prepared collectively for the threats and hazards that pose the greatest risk to the nation. The NPG identifies 32 distinct activities, called core capabilities, needed to address the risks. The NPG organizes these core capabilities into five categories, called mission areas. Some core capabilities apply to more than one mission area. For example, the first three core capabilities—Planning, Public Information and Warning, and Operational Coordination—are cross-cutting capabilities, meaning they apply to each of the five mission areas. The National Preparedness Goal describes the five mission areas as follows:

Prevention

Prevention includes those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. It is focused on ensuring we are optimally prepared to prevent an imminent terrorist attack within the United States. Prevention also includes the intelligence, law enforcement, and homeland defense activities conducted in the event of an act of terrorism in the homeland to determine if follow-on attacks are planned and thwart and/or apprehend the adversary.

Protection

Protection includes capabilities to safeguard the homeland against acts of terrorism and man-made or natural disasters. It is focused on actions to protect the citizens, residents, visitors, and critical assets, systems, and networks against the greatest risks to our Nation in a manner that allows our interests, aspirations, and way of life to thrive. We will create conditions for a safer, more secure, and more resilient Nation by enhancing Protection through cooperation and collaboration with all sectors of society.

Mitigation

Mitigation includes those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. It is focused on the premise that individuals, the private sector, communities, critical infrastructure, and the Nation as a whole are made more resilient when the consequences and impacts, the duration, and the financial and human costs to respond to and recover from adverse incidents are all reduced.

Response

Response includes those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. It is focused on ensuring that the Nation is able to effectively respond to any threat or hazard, including those with cascading effects, with an emphasis on saving and sustaining lives and stabilizing the incident, as well as rapidly meeting basic human needs, restoring basic services and community functionality, establishing a safe and secure environment, and supporting the transition to recovery.

Recovery

Recovery includes those capabilities necessary to assist communities affected by an incident in recovering effectively. It is focused on a timely restoration, strengthening, and revitalization of the infrastructure; housing; a sustainable economy; and the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident. The ability of a

community to accelerate the recovery process begins with its efforts in pre-disaster preparedness, including mitigation, planning, and building capacity for disaster recovery. These efforts result in a resilient community with an improved ability to withstand, respond to, and recover from disasters, which can significantly reduce recovery time and costs.

Core Capabilities by Mission Area

Prevention	Protection	Mitigation	Response	Recovery							
Planning											
Public Information and Warning											
Operational Coordination											
Intelligence and Information Sharing		Community Resilience	Infrastructure Systems								
Interdiction and Disruption			Critical Transportation	Economic Recovery							
Screening, Search and Detection					Environmental Response/Health and Safety	Health and Social Services					
Forensics and Attribution	Access Control and Identity Verification	Long-term Vulnerability Reduction					Fatality Management Services	Housing			
	Cybersecurity								Risk and Disaster Resilience Assessment	Natural and Cultural Resources	
	Physical Protective Measures										Threats and Hazards Identification
	Risk Management for Protection Programs and Activities										
	Supply Chain, Integrity and Security										

Appendix B: Summary of the Core Capabilities

Access Control and Identity Verification

Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

Community Resilience

Enable the recognition, understanding, communication of, and planning for risk to empower individuals and communities to make informed risk management decisions necessary to adapt to, withstand, and quickly recover from future incidents.

Critical Transportation

Provide transportation (including infrastructure access and accessible transportation services) for response priority objectives, including the evacuation of people and animals and the delivery of vital response personnel, equipment, and services into the affected areas.

Cybersecurity

Protect (and, if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Economic Recovery

Return economic and business activities (including food and agriculture) to a healthy state and develop new business and employment opportunities that result in an economically viable community.

Environmental Response/Health and Safety

Conduct appropriate measures to ensure the protection of the health and safety of the public and workers, as well as the environment, from all-hazards in support of responder operations and the affected communities.

Fatality Management Services

Provide fatality management services, including decedent remains recovery and victim identification, working with local, state, tribal, territorial, insular area, and Federal authorities to provide mortuary processes, temporary storage or permanent internment solutions, sharing information with mass care services for the purpose of reunifying family members and caregivers with missing persons/remains, and providing counseling to the bereaved.

Fire Management and Suppression

Provide structural, wildland, and specialized firefighting capabilities to manage and suppress fires of all types, kinds, and complexities while protecting the lives, property, and the environment in the affected area.

Forensics and Attribution

Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source, to include forensic analysis as well as attribution for an attack and the preparation for an attack in an effort to prevent initial or follow-on acts, and/or swiftly develop counter-options.

Health and Social Services

Restore and improve health and social services capabilities and networks to promote the resilience, independence, health (including behavioral health), and well-being of the whole community.

Housing

Implement housing solutions that effectively support the needs of the whole community and contribute to its sustainability and resilience.

Infrastructure Systems

Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

Intelligence and Information Sharing

Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, Federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

Interdiction and Disruption

Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.

Logistics and Supply Chain Management

Deliver essential commodities, equipment, and services in support of impacted communities and survivors, to include emergency power and fuel support, as well as the coordination of access to community staples. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

Long-term Vulnerability Reduction

Build and sustain resilient systems, communities, and critical infrastructure and key resources lifelines to reduce their vulnerability to natural, technological, and human-caused threats and hazards by lessening the likelihood, severity, and duration of the adverse consequences.

Mass Care Services

Provide life-sustaining and human services to the affected population, to include hydration, feeding, sheltering, temporary housing, evacuee support, reunification, and distribution of emergency supplies.

Mass Search and Rescue Operations

Deliver traditional and atypical search and rescue capabilities, including personnel, services, animals, and assets to survivors in need, with the goal of saving the greatest number of endangered lives in the shortest time possible.

Natural and Cultural Resources

Protect natural and cultural resources and historic properties through appropriate planning, mitigation, response, and recovery actions to preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices and in compliance with applicable environmental and historic preservation laws and Executive Orders.

On-scene Security, Protection, and Law Enforcement

Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and also for response personnel engaged in lifesaving and life-sustaining operations.

Operational Communications

Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impacted area and all response forces.

Operational Coordination

Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Physical Protective Measures

Implement and maintain risk-informed countermeasures and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.

Planning

Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical level approaches to meet defined objectives.

Public Health, Healthcare, and Emergency Medical Services

Provide lifesaving medical treatment via Emergency Medical Services and related operations and avoid additional disease and injury by providing targeted public health, medical, and behavioral health support and products to all affected populations.

Public Information and Warning

Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard, as well as the actions being taken and the assistance being made available, as appropriate.

Risk and Disaster Resilience Assessment

Assess risk and disaster resilience so that decision makers, responders, and community members can take informed action to reduce their entity's risk and increase their resilience.

Risk Management for Protection Programs and Activities

Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments.

Screening, Search, and Detection

Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio-surveillance, sensor technologies, or physical investigation and intelligence.

Situational Assessment

Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.

Supply Chain Integrity and Security

Strengthen the security and resilience of the supply chain.

Threats and Hazards Identification

Identify the threats and hazards that occur in the geographic area; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of a community or entity.

Appendix C: Stakeholder Preparedness Review Functional Gaps

* Note: The functional gaps included below by core capability represent the complete list of gaps identified in the 2021 Stakeholder Preparedness Review (SPR). However, inclusion of a functional area in the SPR does not guarantee allowability under the Homeland Security Grant Program (HSGP). All HSGP funded activities must have a terrorism nexus to be allowable.

Planning Core Capability

- Evaluating and updating plans.
- Including individuals with disabilities or access/functional needs.
- Pre-incident planning.
- Incorporating risk analyses.
- Operational planning.
- Integrating different plans.
- Strategic planning.
- Whole community involvement and coordination.

Public Information and Warning Core Capability

- Alerts and warnings.
- Culturally and linguistically appropriate messaging.
- Delivering actionable guidance.
- Developing standard operating procedures for public information.
- New communications tools and technologies.
- Protecting sensitive information.
- Public awareness campaigns.
- Traditional communications mechanisms.

Operational Coordination Core Capability

- Allocating and mobilizing resources.
- Ensuring information flow.
- Ensuring continuity of government and essential services.
- Establishing lines of communication.
- Command, control, and coordination.
- Establishing roles and responsibilities.
- Stakeholder engagement.
- NIMS/ICS compliance.
- Emergency Operations Center management.

Forensics and Attribution Core Capability

- Assessing terrorist capabilities.
- Attribution assessments.
- CBRNE material analysis.
- Crime scene preservation and exploitation.

- Digital media and network exploitation.
- Evidence Collection.
- Forensics analysis.
- Terrorist investigations.

Intelligence and Information Sharing Core Capability

- Establishing intelligence and information requirements.
- Analysis of intelligence and information.
- Continuous threat assessment.
- Safeguarding sensitive information.
- Developing reports and products.
- Disseminating intelligence and information.
- Exploiting and processing information.
- Feedback and evaluation.
- Gathering intelligence.
- Monitoring information.

Interdiction and Disruption Core Capability

- Anti-terrorism operations.
- Border security.
- CBRNE detection.
- CBRNE render safe.
- Wide area search and detection.
- Interdicting cargo, conveyances, and persons.
- Deterrent law enforcement presence.
- Tactical law enforcement operations.
- Tracking and targeting terrorists and their weapons.
- Financial disruption.
- Disease prevention.
- Preventing acquisition of CBRNE.

Screening, Search, and Detection Core Capability

- Electronic search.
- Explosives detection.
- Locating terrorists.
- Physical investigation.
- Wide area search.
- Promoting an observant nation.
- CBRNE detection.
- Radiological and nuclear detection.
- Screening.

- Bio-surveillance.
- Chemical and biological detection.
- Laboratory testing.

Access Control and Identity Verification Core Capability

- Controlling cyber access.
- Controlling physical access.
- Verifying identity.

Cybersecurity Core Capability

- Controlling electronic access.
- Guidelines, regulations, and standards.
- Protective measures.
- Detecting malicious activity.
- Securing CIKR and SCADA systems.
- Sharing threat information.
- Technical countermeasures.
- Continuity of operations for cyber systems.
- Investigating malicious actors.
- End user awareness.

Physical Protective Measures Core Capability

- Biosecurity.
- Border protection.
- Identifying and prioritizing assets to protect.
- Site-specific and process-specific risk assessments.
- Physical Security Measures.

Risk Management for Protection Programs and Activities Core Capability

- Analysis tools.
- Incorporating risk assessments in exercise design.
- Risk communication.
- Risk management planning.

Supply Chain Integrity and Security Core Capability

- Analysis of supply chain dependencies.
- Implementing countermeasures.
- Implementing physical protection.
- Integrating security processes.
- Verification and detection.

Community Resilience Core Capability

- Communication and outreach.
- Education and skill building.
- Understanding the community.
- Collaborative planning and decision-making.
- Partnership building.
- Broadening the use of insurance.

Long-term Vulnerability Reduction Core Capability

- Incorporating mitigation measures into construction and development.
- Individual and family preparedness.
- Adopting vulnerability reduction standards and building codes.
- Developing neighborhood civic organizations.

Risk and Disaster Resilience Assessment Core Capability

- Modeling and analysis.
- Education and training.
- Obtaining and sharing data.

Threat and Hazards identification

- Data collection and sharing.
- Estimating frequency and magnitude.
- Modeling and analysis.
- Stakeholder collaboration/coordination.

Critical Transportation Core Capability

- Debris removal.
- Delivery of response assets.
- Establishing access.
- Evacuation.
- Transportation safety and condition assessments.
- Reentering affected area.
- Airspace management.

Environmental Response/Health and Safety Core Capability

- Hazardous material clean-up.
- Health and safety monitoring and assessment.
- Responder safety.
- Survivor safety and assistance.
- Decontamination.
- Debris removal.

- Environmental impact analysis.
- Predictive modeling.

Fatality Management Services Core Capability

- Bereavement counseling.
- Body recovery.
- Mortuary services.
- Victim Identification.
- Family reunification.

Fire Management and Suppression

- Structural firefighting.
- Extended attack firefighting.
- Initial attack firefighting.
- Specialized firefighting.
- Wildland firefighting.

Logistics and Supply Chain Management

- Access to community staples.
- Donation management.
- Emergency power provision.
- Fuel support.
- Private resources.
- Resource delivery.
- Resource management.
- Resource tracking.
- Supply chain restoration.
- Volunteer management.

Mass Care Services Core Capability

- Relocation assistance.
- Ensuring access.
- Feeding.
- Hydration.
- Pets.
- Resource distribution.
- Family reunification.
- Sheltering.

Mass Search and Rescue Operations Core Capability

- Rescue operations.

- Search operations.
- Specialized operations.
- Synchronizing operations.
- Community-based search and rescue support.

On-scene Security, Protection, and Law Enforcement Core Capability

- Protecting response personnel.
- Securing disaster areas.
- Law enforcement.

Operational Communications Core Capability

- Communication between responders and the affected population.
- Data communications.
- Interoperable communications between responders.
- Re-establishing communications infrastructure.
- Re-establishing critical information networks.
- Voice communications.

Public Health, Healthcare, and Emergency Medical Services Core Capability

- Triage and initial stabilization.
- Emergency Medical Services.
- Definitive care.
- Public health interventions.
- Clinical laboratory testing.

Situational Assessment Core Capability

- Assessing hazard impacts.
- Stakeholder engagement.
- Tracking response activities.
- Analyzing information.
- Delivering situation reports.

Infrastructure Systems Core Capability

- Communications systems.
- Dams and flood control.
- Food production and delivery.
- Government facilities.
- Heating fuel provision.
- Hospitals.
- Infrastructure site assessments.
- Power restoration.

- Sanitation.
- Public recreation facilities.
- Public safety facilities.
- Transportation infrastructure.
- Water treatment and provision.

Economic Recovery Core Capability

- Business/economic continuity planning.
- Developing the workforce.
- Economic impact assessments.
- Disseminating information.
- Incentivizing entrepreneurial and business development.
- Management planning.
- Reopening businesses.
- Developing recovery objectives.

Health and Social Services Core Capability

- Behavioral health.
- Ensuring access.
- Environmental health.
- Healthcare facilities and coalitions.
- Social services.
- School impacts.
- Medical products and services.

Housing Core Capability

- Addressing housing shortages.
- Housing accessibility.
- Housing affordability.
- Housing assessments.
- Transition from interim to permanent/long-term housing.
- Reconstruction of destroyed housing.
- Rehabilitation of damaged housing.

Natural and Cultural Resources Core Capability

- Damage assessment.
- Environmental preservation and restoration.
- Historic preservation.

Appendix D: FY 2022 Programs - Allowable Program Activities

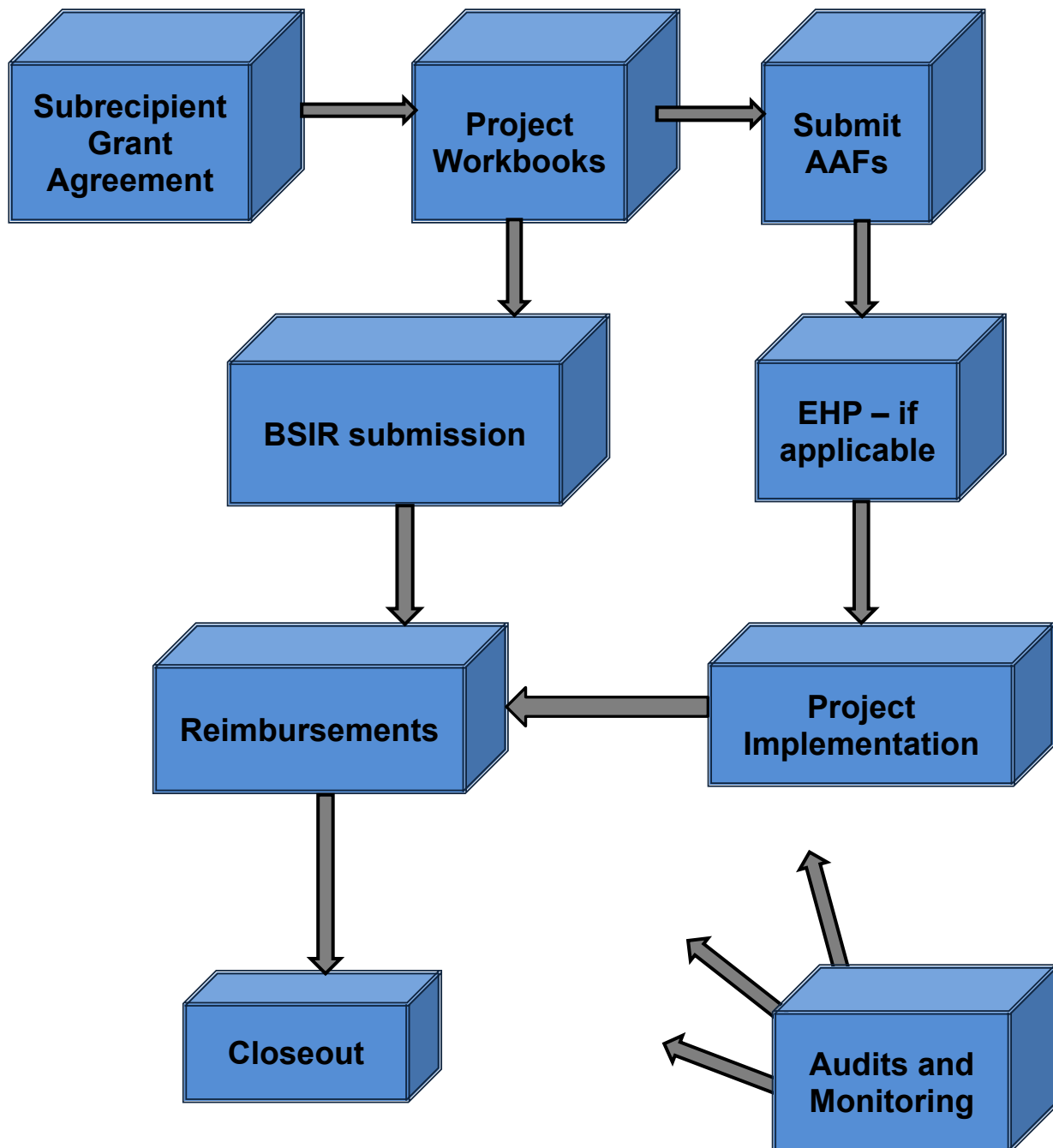
Allowable Program Activities Current as of FY 2022 Programs	SHSP	UASI	OPSG
This list is not all-inclusive. See the respective program guidance for additional details and/or requirements			
Allowable Planning Costs			
Developing hazard/threat-specific annexes	Y	Y	N
Developing and implementing homeland security support programs and adopting ongoing FEMA national initiatives	Y	Y	N
Developing related terrorism and other catastrophic event prevention activities	Y	Y	N
Developing and enhancing plans and protocols	Y	Y	N
Developing or conducting assessments	Y	Y	N
Hiring of full- or part-time staff or contract/consultants to assist with planning activities	Y	Y	N
Materials required to conduct planning activities	Y	Y	N
Travel/per diem related to planning activities	Y	Y	Y
Overtime and backfill costs (in accordance with operational Cost Guidance)	Y	Y	Y
Issuance of WHTI-compliant Tribal identification cards	Y	N	N
Activities to achieve planning inclusive of people with disabilities and others with access and functional needs and limited English proficiency.	Y	Y	N
Coordination with Citizen Corps Councils for public information/education and development of volunteer programs	Y	Y	N
Update governance structures and processes and plans for emergency communications	Y	Y	N
Development, and review and revision of continuity of operations plans	Y	Y	N
Development, and review and revision of the THIRA/SPR continuity of operations plans	Y	Y	N
Allowable Organizational Activities			
Note: Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.			
Program management	Y	Y	N
Development of whole community partnerships	Y	Y	N
Structures and mechanisms for information sharing between the public and private sector	Y	Y	N
Implementing models, programs, and workforce enhancement initiatives	Y	Y	N
Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors	Y	Y	N
Operational support	Y	Y	N
Utilization of standardized resource management concepts	Y	Y	N
Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS), or needs in resulting from a National Special Security Event	Y	Y	N
Reimbursement for select operational expenses associated with increased security measures at critical infrastructure sites incurred (up to 50 percent of the allocation)	Y	Y	Y

Overtime for information, investigative, and intelligence sharing activities (up to 50 percent of the allocation)	Y	Y	Y
Hiring of new staff positions/contractors/consultants for participation in information/intelligence analysis and sharing groups or fusion center activities (up to 50 percent of the allocation).	Y	Y	N
Allowable Equipment Categories			
Personal Protective Equipment	Y	Y	Y
Explosive Device Mitigation and Remediation Equipment	Y	Y	N
CBRNE Operational Search and Rescue Equipment	Y	Y	N
Information Technology	Y	Y	Y
Cybersecurity Enhancement Equipment	Y	Y	N
Interoperable Communications Equipment	Y	Y	Y
Detection	Y	Y	Y
Decontamination	Y	Y	N
Medical countermeasures	Y	Y	Y
Power (e.g., generators, batteries, power cells)	Y	Y	Y
CBRNE Reference Materials	Y	Y	N
CBRNE Incident Response Vehicles	Y	Y	N
Terrorism Incident Prevention Equipment	Y	Y	Y
Physical Security Enhancement Equipment	Y	Y	Y
Inspection and Screening Systems	Y	Y	Y
Animal Care and Foreign Animal Disease	Y	Y	N
CBRNE Prevention and Response Watercraft	Y	Y	N
CBRNE Prevention and Response Unmanned Aircraft	Y	Y	N
CBRNE Aviation Equipment	Y	Y	N
CBRNE Logistical Support Equipment	Y	Y	N
Intervention Equipment (e.g., tactical entry, crime scene processing)	Y	Y	Y
Critical emergency supplies	Y	Y	N
Vehicle acquisition, lease, and rentals	N	N	Y
Other Authorized Equipment	Y	Y	Y
Allowable Training Costs			
Overtime and backfill for emergency preparedness and response personnel attending DHS/FEMA-sponsored and approved training classes	Y	Y	Y
Overtime and backfill expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA training	Y	Y	Y
Training workshops and conferences	Y	Y	Y
Activities to achieve training inclusive of people with disabilities and others with access and functional needs and limited English proficiency	Y	Y	N
Full- or part-time staff or contractors/consultants	Y	Y	Y
Travel	Y	Y	Y
Supplies	Y	Y	N
Instructor certification/re-certification	Y	Y	N
Coordination with Citizen Corps Councils in conducting training exercises	Y	Y	N
Interoperable communications training	Y	Y	N
Activities to achieve planning inclusive of people with limited English proficiency	Y	Y	N
Immigration enforcement training	Y	Y	Y
Allowable Exercise Related Costs			
Design, Develop, Conduct, and Evaluate an Exercise	Y	Y	N
Full- or part-time staff or contractors/consultants	Y	Y	N
Overtime and backfill costs, including expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA	Y	Y	N

exercises			
Implementation of HSEEP	Y	Y	N
Activities to achieve exercises inclusive of people with disabilities and others with access and functional needs	Y	Y	N
Travel	Y	Y	N
Supplies	Y	Y	N
Interoperable communications exercises	Y	Y	N
Activities to achieve planning inclusive of people with limited English proficiency	Y	Y	N
Allowable Management and Administrative Costs			
Hiring of full- or part-time staff or contractors/consultants to assist with the management of the respective grant program, application requirements, and compliance with reporting and data collection requirements	Y	Y	Y
Development of operating plans for information collection and processing necessary to respond to DHS/FEMA data calls	Y	Y	Y
Overtime and backfill costs	Y	Y	Y
Travel	Y	Y	Y
Meeting related expenses	Y	Y	Y
Authorized office equipment	Y	Y	N
Recurring expenses such as those associated with cell phones and faxes during the PoP of the grant program	Y	Y	N
Leasing or renting of space for newly hired personnel during the PoP of the grant program	Y	Y	N
Law Enforcement Terrorism Prevention Activities (LETPA) Costs			
Integration and interoperability of systems and data, such as CAD and RMS, to facilitate the collection, evaluation, and assessment of suspicious activity reports, tips/leads, and online/social media-based threats.	Y	Y	N
Maturation and enhancement of designated state and major Urban Area fusion centers	Y	Y	N
Coordination between fusion centers and other analytical and investigative efforts	Y	Y	N
Implementation and maintenance of the Nationwide SAR Initiative	Y	Y	N
Implementation of the "If You See Something, Say Something®" campaign	Y	Y	N
Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical	Y	Y	N
Building and sustaining preventive radiological and nuclear detection capabilities	Y	Y	N

Appendix E: Subrecipient Administrative Process

This appendix is provided as a quick overview of the administrative processes and requirements of subrecipient HSGP grant awards. This is not an exhaustive inventory of all potential HSGP administrative requirements, and some projects may include additional evaluation or reporting requirements.



Appendix F: FY 2022 HSGP Project Workbook Checklist

Checking the following steps before the submission deadline will help ensure that projects pass federal review.

Workbook Checkpoints

- I. Project Fields
- II. Alignment
- III. Shareable or Deployable
- IV. Funding
- V. LETPA
- VI. Milestones
- VII. Project Descriptions
- VIII. Sustain/NIMS/Construction

Tab A

- ☐ **I:** All project fields are complete. (Example: Subrecipient Name, Zip Code...)
- ☐ **II:** Is most appropriate core capability selected?
- ☐ **II:** Is project aligned to correct investment as determined by core capability?
- ☐ **II:** Check Core Capability alignment with Investment. (Example: SHSP-5 -CBRNE Response Capabilities / Mass Search and Rescue Operations)
- ☐ **III:** Check if Shareable and Deployable responses are accurate.
- ☐ **Shareable**
Provides information on the utility of a non-deployable shared asset in a region; identifies the asset's ability to augment and sustain a reinforced response within a region. An asset that can be utilized as a local, state, regional, or national capability, but is not physically deployable (i.e., fusion centers).

OR (*Can be neither but **cannot** be both*)
- ☐ **Deployable**
Identifies the availability and utility of an asset to multiple jurisdictions, regions, and the Nation; provides information on mobility of assets in an area. An asset that is physically mobile and can be used anywhere in the United State and territories via EMAC or other mutual aid/assistance agreements.
- ☐ **IV:** Check that Investment is aligned with appropriate funding source.
- ☐ **IV:** Ensure allocation of Solution Areas fits within Project Description. (Example: Planning for a conference should have allocation of funds in Planning).
- ☐ **V:** Does the Regional Grant total allocation have 30% of funding dedicated towards LETPA?

- ☐ **V:** If project includes LETPA, ensure project capabilities are allowable LETPA activities.

All Core capabilities under the Prevention and Protection Mission Area are LETPA-eligible and some core capabilities under other Mission Areas are possible.

- ☐ **VI:** Milestones should include more than one and must cover the entire implementation of the project to be funded with the applicable grant year funds.
- ☐ **VI:** Can the project be completed within the period of performance?

Tab B

- ☐ **VII:** Check if Project Description aligns with Investment which will be determined by the Core Capability.
 - ☒ *M&A project included.*
- ☐ **VII:** Is adequate detail provided?
- ☐ **VII:** Are specific core capability gaps identified?
- ☐ **VII:** Does project description support funding request?
- ☐ **VIII:** Ensure Core Capability is within Project Description and specific gaps are identified. (Example: Provide power restoration systems to government facilities, public safety facilities, and shelters. This project supports the infrastructure Systems core capability in the following functional areas identified in the SPR: communications systems, government facilities, power restoration, and public safety facilities.

Tab C

- ☐ **VIII:** If the project is sustainment, make sure the column, “Last completed milestone of the previous investment” is completed with previous investment information pertaining to that project.
- ☐ **VIII:** Ensure NIMS fields are completed if the project supports a NIMS capability.
- ☐ **VIII:** Verify Construction Activity with Project Description.

References

Building Capability/Sustaining Capability

Building refers to activities that start a new capability or increase a capability. Sustaining refers to activities that maintain a capability at its current level. This project attribute contributes to the risk and gap analysis of the applicant and the Federal reviewers. It will assist FEMA in measuring progress towards the National Preparedness Goal.

Resource Typing

As part of the description for each project, the applicant must identify whether the project supports a NIMS-typed resource. Applicants should refer to the Resource Typing Library Tool located at <http://www.fema.gov/resource-management> to select specific typed resources. Resource typing is categorizing, by capability, the resources requested, deployed, and used in incidents. Measurable standards identifying resource capabilities and performance levels serve as the basis for categories. Resource users at all levels use these standards to identify and inventory resources. Resource kinds may be divided into subcategories to define more precisely the capabilities needed to meet specific requirements.

Appendix G: FY 2022 Homeland Security Grant Program Document Submission Checklist

- ☐ **Fiscal Year (FY) SHSP/UASI Grant Agreement– Est. November 27, 2022** (varies each year, exact date will be included with the grant agreement package). Return the following documents: one signed grant agreement; Subrecipient Risk Assessment Certification; Standard Assurances; Certifications Regarding Lobbying, Debarment, Suspension and Other Responsibility Matters; Audit Certification; and Taxpayer Identification Number and Certification (W-9).
- ☐ **FY 2022 National Priority Area Projects – November 15, 2022.** Any additional or replacement projects (including any changes in the funding amount) supporting one of the national priority area funding requirements must be submitted to FEMA for subject matter expert review.
- ☐ **FY 2022 SHSP/UASI Project Workbooks – October 30, 2022.** Project Workbooks must be updated with actual FY 2022 funding levels for submission in the federal Grants Reporting Tool.
- ☐ **Biannual Strategy Implementation Report (BSIR) – April 30 and October 30 every year.** The BSIR is a federal reporting requirement that must account for all grant funds and provide an update on the progress of your projects. The submission due on April 30 should reflect activities between October 1-March 31 of the previous year. The October 30 report should reflect activities from April 1 to September 30.
- ☐ **Project workbooks – April 30 and October 30 every year.** An updated project workbook must be submitted with each BSIR submission.
- ☐ **Fiduciary Identification - August 31, 2022 –** The FY 2022 HSGP regional fiduciary must be identified and submitted to MSP/EMHSD.
- ☐ **Alignment and Allowability Forms (AAF's) - Ongoing as needed throughout grant.** The AAF must align to a project included in the project workbook. Cost eligibility determination is based on information provided in the AAF, including the intended use/outcome of the project, and assessed against grant program guidance.
- ☐ **Environmental and Historic Prevention (EHP) Screening Form – As needed, determined by project.** An EHP must be approved by FEMA before a project can start. If an EHP is required, notice will be sent by MSP/EMHSD after receipt of the AAF. The AAF approval is conditional upon completing an EHP and receiving FEMA approval. The AAF will not be returned to the subrecipient until after EHP approval is received.
- ☐ **Reimbursements - No later than 30 days following the end of the subrecipient period of performance.** Must include Reimbursement cover sheet (EMD-054), approved AAF with page 5 completed; proof of payment; and paid invoice; EHP approval, EMD-056 Equipment, Supplies and Other Items Reimbursement Detail, or EMD-055 Payroll Reimbursement Detail, as applicable.

- ☐ **Personnel Certifications – Nov. 1st and April 30th (every year).** All HSGP funded personnel (M&A included) are required to have a current personnel certification form on file.
- ☐ **Nationwide Cybersecurity Review – Suggested December 31, 2022.** The Nationwide Cybersecurity Review is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of state, local, tribal, and territorial governments' cybersecurity programs. All direct beneficiaries of HSGP funded projects must participate in the survey. The suggested deadline is December 31, 2022. However, the assessment tool will be open until February 28, 2023.
- ☐ **Equipment Inventory List – June 30, 2023, and every odd year thereafter.** If equipment is purchased, as defined by 2 CFR 200, it must be maintained in an equipment inventory list that includes specific information outlined in 2 CFR 200.313 and a physical inventory reconciled to that list must be completed once every two years. The reconciled equipment inventory list must be submitted to MSP/EMHSD by **July 31, 2023, and every odd year thereafter.**
- ☐ **Grant Files – 3 years after grant closeout.** Subrecipients must maintain all grant documentation for three years following the closeout of the grant. Records must be available upon request for state or federal audit.
- ☐ **Equipment Records – 3 years after disposition.** Subrecipients must maintain all equipment documentation for three years following disposition of the equipment. Records must be available upon request for state or federal audit.

Appendix H: Discussion on 2 CFR Part 200 Compliance Issues

As the State Administrative Agency (SAA) for the Federal Emergency Management Agency preparedness grant programs, the Michigan State Police/Emergency Management and Homeland Security Division (MSP/EMHSD) is responsible for ensuring that all subrecipients adhere to requirements established by the Federal government laid out in the Code of Federal Regulations (CFR).

The Uniform Administrative Requirements, Cost Principles, and Audit Requirements governing all Federal grants are contained in 2 CFR 200 and Appendix II, both of which can be found at www.ecfr.gov. Resources designed to assist subrecipients in complying with the 2 CFR 200 requirements are located on the MSP/EMHSD Grant Programs webpage found by entering www.michigan.gov/emhsd in your browser; click Grant Programs in the left margin, then click on your grant. For procurement resources, click the word "Procurement".

MSP/EMHSD monitors grant compliance and provides guidance on how to best implement the Federal requirements. The following is an overview of some of the 2 CFR 200 requirements that are common areas where mistakes can be made. Subrecipients are encouraged to contact their agency's legal staff for assistance on compliance concerns.

PROCUREMENT

The Procurement Procedures (2 CFR 200.318-327 and Appendix II) have been a focus of FEMA and recent Office of Inspector General (OIG) audits. If you want to read a specific citation, enter ecfr.gov in your browser, click the down arrow in the box, select Title II and click "Go", click "200-299", click "200", then scroll to the citation you are looking for and click.

The following are important procurement points to understand.

In all procurements, you must follow your organization's procurement policy unless Federal regulations or local laws and regulations are more restrictive. (2 CFR 200.318 (a))

The following is a list of resources found under Procurement on the MSP/EMHSD Grant Programs webpage:

- FEMA Contract Provisions Template
- Contract Criteria Table
- Quick Reference Table for FEMA Contract Provisions Template
- Davis-Bacon and Related Acts (DBRA) Fact Sheet
- Instructions for Creating the Wage Determination Document for Contracts
- Instructions for Checking for Excluded and Debarred Contractors
- SBA Search Tool Quick Reference Guide
- Top 10 Procurement Mistakes

"Buy Local" Provision in Subrecipient Procurement Requirements (2 CFR 200.319 (c))

You are not allowed to enforce geographically limiting provisions of your local procurement policy for Federal grant funded procurement.

Situation:

The subrecipient's jurisdiction enforces the "Buy Local" provision in their ordinances for all procurement. Consequently, during a Federal-grant funded procurement process, only vendors from within 100-miles of the jurisdiction were considered.

Results:

Not allowed. You may not restrict competition in procurement by enforcing geographic or other limiting preferences.

Suggestion:

Publicly advertise the solicitation and include at least one socio-economic vendor. Vendors meeting the geographic limitations may respond; however, if selected you will want to clearly document that the selection was not made because of their geographic location but for other reasons. Those details must be clearly documented in the procurement files.

Contract Provisions (2 CFR 200.327 and Appendix II)

All subrecipients are required to prepare a document that includes the required contract provisions listed in 2 CFR 200.327 and Appendix II.

FEMA has prepared a Contract Provisions Template that lists all the required and recommended provisions, an explanation of each one, and required or suggested language to be used. MSP/EMHSD has prepared the following documents, located on the Grant Programs webpage, to help navigate the FEMA Contract Provisions Template, also located on the Grant Programs webpage.

Contract Criteria – lists the provisions in order of criteria requiring the provision. Some provisions are required for all contracts, others have dollar thresholds that must be met before the provision is required.

Quick Reference Table for FEMA's Contract Provision Template – will help you locate the page in the FEMA Contract Provisions Template where the suggested or required language is located.

If your project is a construction project, the Davis Bacon Act may come into play. One of the requirements of this act is to provide a Wage Determination Document with all solicitations.

Instructions for Creating the Wage Determination Document – explains how to create the Wage Determination document.

Noncompetitive Procurement (Sole Sourcing) (2 CFR 200.320 (c))

MSP/EMHSD discourages all forms of noncompetitive procurement. Sealed bids or other methods of procurement solicitation should be used even in situations where you believe only one vendor can supply the goods or services. Subrecipients must discuss the noncompetitive procurement situation with the appropriate MSP/EMHSD personnel prior to this type of procurement activity.

Socio-Economic Procurement (2 CFR 200.321)

Subrecipients are required to include at least one socio-economic vendor for all procurement solicitations. We recommend documenting the socio-economic vendor solicited and how you know them to be a socio-economic vendor.

Situation: A subrecipient searched for a socio-economic vendor within 100 miles of their location. They could not find any that could provide the service they needed. They documented their efforts and selected a vendor who responded to the solicitation.

Results:

Not allowed. Subrecipients must include at least one socio-economic vendor, regardless of their geographic location, in all procurement solicitations.

Suggestion: The Small Business Association has developed a database to assist in locating socio-economic businesses called the Dynamic Small Business Search. The SBA Search Tool Quick Reference Guide, located on the MSP/EMHSD Grant Programs webpage, will walk you through the steps of navigating this database. It is important that your search criteria are broad enough so that at least one socio-economic firm is identified. If you have response-time concerns based on the distance of the firm's location to you, include those requirements in your solicitation. It is up to the firm to decide if they can meet the criteria. In order to comply with 2 CFR 200.321, you must ensure your search is broad enough to include at least one socio-economic firm.

Suspension and Debarment (2 CFR 200.205 (d) and Appendix II (H))

Subrecipients are required to check whether their potential contractor(s) are suspended or debarred from doing business with the Federal government. Instructions for accessing www.SAM.gov are found on the Grant Program website.

Instructions for Checking for Excluded & Debarred Contractors – lists detailed instructions for checking and documenting whether contractors are suspended or debarred.

Situation: The subrecipient did not check www.SAM.gov to ensure the contractor they selected was not listed as being suspended or debarred from doing business with the Federal government. The contractor was suspended on www.SAM.gov.

Results:

Not allowed, and contractor may not be used.

Suggestions: Follow the instructions for checking for excluded and debarred contractors, make a print screen of the results, and keep in your procurement files for that project. If the contractor is suspended or debarred, do not engage in any form of procurement with that contractor.

GENERAL COMPLIANCE TOPICS

Conflict of Interest (2 CFR 200.318 (c) (1))

A conflict of interest is present when anyone from your organization is involved in any part of a procurement process or supervision of a vendor that has any kind of a relationship with any person directly or indirectly related to the potential vendor.

Situation: A subrecipient is considering a procurement. The brother of a board member is a salesman for one of the vendors being considered. The board-member is asked about his brother's work ethic and stability of his company. The board decides to go with the brother's firm because they were the low bid.

Results:

Not allowed. Even though the vendor's bid was the lowest, the conflict-of-interest relationship of the board member and a member of the vendor's company negates that company from being eligible for being considered.

Suggestion:

When the discussion began and the board member knew that his brother might be a candidate for the solicitation, that board member should have recused himself from the process and not be involved with any aspect of the project, including supervision of the contractor.

Another suggestion would be to not consider the company at all to ensure there is no perception of impropriety. Subrecipients must remember, even if there is no factual impropriety, if there could be a perception of impropriety, the action should be avoided.

Dual Compensation (5 U.S. Code §5533 and Federal Grant Guidance)

Employees who work for Federal, state, or local agencies are paid with taxpayer dollars. These employees cannot be paid from another taxpayer-supported funding source for work performed while they are receiving taxpayer-funded wages, which includes annual leave, sick time, holidays, or any other paid time off.

Situation: An employee working for a jurisdiction and paid, in part, by the EMPG grant is asked to teach an ICS course at the Emergency Management and Homeland Security Training Center in Lansing (for pay). This employee plans to take vacation time from their every-day job for the days they will be teaching.

Results:

Not Allowed. This situation represents dual compensation. The employee is getting paid by their jurisdiction (vacation pay) for the same time period they are getting paid to teach.

Suggestion: The employee could switch their pass days or request unpaid leave for the teaching days.

Equipment Procedures (2 CFR 200.313)

Equipment purchased with a per-item cost of \$5,000 or more (or your organization's capitalization level for financial statement purposes if less than \$5,000) must be put on a list that contains specific identifying information about the equipment. In addition, a physical inventory of the equipment shall be performed and reconciled to the list every two years. The document *Equipment Definitions* can be found on the Grant Programs webpage in the Guidance and Resources section.

Situation: The subrecipient is not maintaining adequate property records and/or has not conducted and documented a physical inventory of equipment within the past two years.

Results:

Not allowed. If an item of equipment meets any of the definitions in the *Equipment Definitions* document, you must maintain an equipment inventory list for those purchases and complete a physical inventory every two years.

Suggestion: The subrecipient prepare an equipment inventory list using the template found on the MSP/EMHSD Grant Program webpage under Guidance and Resources. You are not required to use the template; however, your list must contain all of the required information. Additionally, beginning in 2021 and every odd year thereafter, the subrecipient must perform a

physical inventory and update the list by June 30. A copy of the equipment inventory must be submitted to the MSP/EMHSD Audit Unit by July 31 every odd year, beginning 2021.

Personnel Activity Reporting Requirements (2 CFR 200.430 (i) (1) (i-x))

Subrecipients must have a position description and maintain activity reports for employees and contractors paid with Federal grant funds. These reports must be sufficient to identify the worker, date, all funding sources, the task performed in such detail that a reviewer would be able to understand the task performed, time to complete the tasks by funding source, and total hours worked for the day. If more than one funding source, care must be exercised to ensure there is no dual compensation.

Situation: A planner paid with HSGP grant funds completes a timecard weekly that is signed by a supervisor. This planner does not have a position description identifying the tasks to be completed, and there is no record of the work performed during the pay period.

Results:

Not allowed. All employees and contractors must have a position description and some sort of personnel activity report that details the required information identified above. Tasks performed must be recorded in adequate detail so a determination of the allowability of the task can be ascertained by a reviewer.

Suggestion: A position description for the employee or contractor position must be prepared and appropriately approved. The subrecipient should create and require completion of a personnel activity log that captures the employee or contractor's name, date, tasks performed in sufficient detail, time associated with the tasks, and total time worked for the day. Periodically, the tasks should be compared to the position description to ensure the employee or contractor is completing the job outlined in the position description. If the employee or contractor is paid by more than one funding source, activities from all funding sources should be captured on the personnel activity log. There should be an indication that a supervisory person reviewed the log.

Single Audit Requirement and Subrecipient Monitoring (2 CFR 200.501 (a) and 200.331 (f))

If the subrecipient organization has Federal grant expenditures of \$750,000 or more from all Federal sources in a fiscal year, they are required to have a single audit conducted. In addition, if you are a pass-through entity, you are required to monitor your subrecipients for the single audit requirement, review any single audit findings pertaining to MSP/EMHSD passed-through grants, and follow-up on the corrective action for the finding.

Situation: A subrecipient (who has subrecipients) has expended more than \$750,000 in Federal grant awards. They have a single audit conducted, and there are no audit findings. However, one of their subrecipients, also expending \$750,000 in Federal awards, has a single audit conducted and audit findings pertaining to MSP/EMHSD grants are reported. The subrecipient did not know of these findings.

Results:

Not allowed. Subrecipients are required to monitor their subrecipients to ensure the single audit requirement is followed and there are no findings pertaining to the passed-through grants.

Suggestion: The subrecipient should maintain a list of their subrecipients, identifying those who are required to have a single audit. Annually, their subrecipient's single audit report should be reviewed for findings pertaining to MSP/EMHSD passed-through grants. If there are findings, the Agency Response should be reviewed, and a determination made as to whether the corrective action will correct the situation causing the finding.

Appendix I: Advance Request Procedures

If necessary, your organization may request an advance of grant funds by following the requirements below.

Advance Request Conditions

- Requests for advances must be for \$10,000 or more.
- The advance must be requested in a formal letter and include all documentation listed below together in an advance request packet.
- Advance funds must be placed in an interest-bearing account.
- Any interest earned over \$500 must be returned to MSP/EMHSD.
- All invoices and proof of payment must be dated and submitted to MSP/EMHSD within 90 days of receipt of the advance.
- All goods and services must be received within 60 days of receipt of the advance to ensure the 90-day advance liquidation deadline is met.

Advance Request Packet Required Documentation

- All advances must be requested in a formal letter, attached via email. The letter must include the following:
 - Grant program title and grant year.
 - Dollar amount of advance request.
 - A line-item budget including each item to be purchased with the advanced funds.
 - Certification that goods and services will be received within 60 days of receiving the advanced funds and proof of payment will be dated and submitted to MSP/EMHSD within 90 days of receipt of advance funds.
 - Advance request letters omitting any of the above criteria will not be considered.
- Approved purchase order(s).
- Vendor's quote/invoice.
- Signed and approved Alignment and Allowability Form (AAF).

Storage of Advance Funds

- Subrecipient must place advanced funds in an interest-bearing account.
- Subrecipient may keep interest earned up to \$500 per year to cover administrative expenses for all federal grant funds combined.
- Subrecipient must notify the MSP/EMHSD quarterly, in writing, of any interest earned over \$500.
- Subrecipients must send the MSP/EMHSD a check payable to the State of Michigan for any interest earned over \$500.
- Interest received by the MSP/EMHSD is returned to the federal government.

Advance Timeframe

Advances cannot be outstanding for longer than 90 days. All invoices and proof of payment must be dated within 90 days of the advanced payment issue date.

When advance purchases are completed, subrecipient must submit:

- Reimbursement cover sheet (EMD-054) and indicate it is advance documentation.
- Copy of supporting paid invoices.
- Copy of cancelled checks.
- Copy of approved alignment and allowability form (AAF).
- A check for unused portion of advance made payable to the State of Michigan.
- Details forms (if necessary).

Example of Advance Request Letter

Date

First and Last Name, Departmental Analyst
Financial Management and Audit Section
State Police Emergency Management and Homeland Security

RE: Advance of FY XX HSGP SHSP/UASI (LETPA) Eligible Funds in the amount of
\$XX,XXX.XX

As fiduciary of the Region X, I am requesting an advance of \$XX,XXX.XX for a
(Equipment/Supplies, etc.) project.

The advance funds will be used to pay for (explanation). The Purchase Order, Vendor's quote
and approved AAF are attached.

The purchase/items will be received and completed within 60 days of Region X receiving the
advance.

Sincerely,

Signature

Name
Title
Agency

Attachments(#)

Appendix J: Acronym List

AAF	Alignment and Allowability Form
AEL	Authorized Equipment List
BSIR	Biannual Strategy Implementation Report
CBRNE	Chemical, Biological, Radiological, Nuclear or Explosive
CFR	Code of Federal Regulations
CIKR	Critical Infrastructure and Key Resources
COC	Critical Operational Capabilities
CPG	Comprehensive Preparedness Guide
EHP	Environmental and Historic Preservation
EIN	Employer Identification Number
EMAC	Emergency Management Assistance Compact
EMAP	Emergency Management Accreditation Program
EOP	Emergency Operations Plan
GPD	Grant Program Directorate
HSGP	Homeland Security Grant Program
IB	Information Bulletin
IJ	Investment Justification
JTTF	Joint Terrorism Task Force
LETPA	Law Enforcement and Terrorism Prevention Activities
M&A	Management and Administration
MIOC	Michigan Intelligence Operations Center
NIMS	National Incident Management System
NOFO	Notice of Funding Opportunity
NPG	National Preparedness Goal
NPS	National Preparedness System
OPSG	Operations Stonegarden
POETE	Planning, Organization, Equipment, Training, and Exercises
PoP	Period of Performance
SAA	State Administrative Agency
SAR	Suspicious Activity Reporting
SHSP	State Homeland Security Program
SPR	Stakeholder Preparedness Review
THIRA	Threat and Hazard Identification and Risk Assessment
UASI	Urban Areas Security Initiative

Appendix K: MSP/EMHSD Points-of-Contact

Subject Matter	POC	Phone	Email
Audit / Site Visit	Ms. Sherrie Loader	517-285-7495	LoaderS@michigan.gov
District Coordinator, Region 1	Lt. Jeffery Yonker	517-719-9767	YonkerJ@michigan.gov
District Coordinator, Region 2N	Lt. Timothy Ketvirtis	517-202-5597	KetvirtisT@michigan.gov
District Coordinator, Region 2S	Lt. Lamarr Johnson	248-508-9171	JohnsonL30@michigan.gov
District Coordinator, Region 3	Lt. Charles Barker	810-223-8466	BarkerC@michigan.gov
District Coordinator, Region 5	Lt. Joshua Collins	517-202-5545	CollinsJ1@michigan.gov
District Coordinator, Region 6	Lt. Orville Theaker	269-953-6099	TheakerO@michigan.gov
District Coordinator, Region 7	Lt. Michael DeCastro	231-499-8266	DecastroM@michigan.gov
District Coordinator, Region 8	Lt. Steven Derusha	517-898-5055	DerushaS1@michigan.gov
HSGP Program Analyst	Ms. Daniele Asbridge	517-388-7619	AsbridgeD@michigan.gov
HSGP Program Analyst	Mr. Michael Graff	517-614-3638	GraffM2@michigan.gov
HSGP Program Analyst	Mr. Paul Lounsberry	517-256-3920	LounsberryP@michigan.gov
HSGP Financial Analyst	Ms. Mikaela Lodes	517-388-8567	LodesM1@michigan.gov
HSGP Financial Analyst	Ms. Amanda VanKoeving	517-388-8569	VanKoevingA@michigan.gov
Financial Administration Unit Manager	Ms. Tammy Eaton	517-230-7497	EatonT@michigan.gov
Risk Reduction and Recovery Section Manager	Ms. Penny Burger	517-898-0551	BurgerP@michigan.gov
Preparedness Grants Unit Manager	Ms. Kim Richmond	517-204-0211	RichmondK@michigan.gov
NIMS Compliance	Mr. Henrik Hollaender	517-898-4225	HollaenderH@michigan.gov
Training	Ms. Danica Frederick	517-285-9714	FrederickD3@michigan.gov
Exercise	Ms. Deanna Johnston	517-648-8689	JohnstonD3@michigan.gov
Project Submittals	EMD_HSGP@michigan.gov	N/A	EMD_HSGP@michigan.gov